

PointSystem™
Media Conversion Center™

CPSMC1900-100

USER'S GUIDE

(revision B)

COMPLIANCE INFORMATION

UL Listed

C-UL Listed (Canada)

CISPR22/EN55022 Class A + EN55

CE Mark

FCC Regulations

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

Canadian Regulations

This digital apparatus does not exceed the Class A limits for radio noise for digital apparatus set out on the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

European Regulations

Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Achtung !

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention !

Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées



CAUTION: RJ CONNECTORS ARE NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentliches Telekommunikationsnetz in den EG-Mitgliedstaaten verstösst gegen die jeweiligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Trademark Notice

All registered trademarks and trademarks are the property of their respective owners.

Copyright Restrictions

© 2001-2003 TRANSITION Networks.

All rights reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical – without written permission from TRANSITION Networks.

Printed in the U.S.A.

33242.B

Table of Contents

1.	INTRODUCTION	1.1
1.1	The Media Conversion Center	1.2
1.1.1	AC Power Supply Module	1.2
1.1.2	Optional Redundant AC Power Supply Module	1.3
1.1.3	Optional 48-VDC Power Supply Module	1.3
1.1.4	Optional LED Slide-in-Module	1.4
1.1.5	Media Converter Slide-in-Modules	1.4
1.2	Optional Network Management	1.5
1.2.1	Management Module(s)	1.5
1.2.2	SNMP Agent in Base Management Module	1.7
	Serial-port DB-9 Connection	1.7
	Network RJ-45 Connection	1.7
1.2.3	Management Software at Command-line Interface	1.8
	CLI Access via Serial Port	1.8
	CLI Access via Telnet	1.9
1.2.4	PointSystem™ Network Security	1.10
	Password Protection	1.10
	Remote Telnet Access Configuration	1.10
	SNMPLock Command	1.11
	Console Lock Command	1.11
1.2.5	PointSystem™ Web-Based Management	1.12
1.2.6	FocalPoint™ Software at Remote NMS	1.13
2	INSTALLATION	2.1
2.1	Unpacking CPSMC1900 Equipment	2.2
2.2	Installing Optional Management Module in Media Conversion Center Chassis	2.3
2.3	Installing Selected Media Converter Slide-in-Module(s) in Media Conversion Center Chassis	2.5
2.4	Installing Optional Power Supply Module	2.6
2.4.1	Setting Master/Slave-Management/Manual Switch	2.7
2.4.2	Securing Power Supply Module to Chassis	2.9
2.5	Installing Optional Fan Module	2.10

2.6	Installing Media Conversion Center at Site	2.11
2.6.1	Standard 19-Inch Rack Installation	2.11
2.6.2	Table-Top Installation	2.12
2.7	Optionally Cascading Management Modules	2.13
2.8	Connecting Media Converter Slide-In-Modules to Network	2.14
2.9	Powering the Media Conversion Center	2.15
2.9.1	Through the AC Power Supply Module	2.15
2.9.2	Through the 48-VDC Power Supply Module	2.16
2.10	Optionally Configuring Network Management	2.17
2.10.1	Network Security	2.17
	Password Protection	2.17
	Remote Telnet Access Configuration	2.17
	SNMPLock Command	2.18
	Console Lock Command	2.18
2.10.2	Setting IP Parameters at Attached Terminal	2.19
	Attaching Terminal or Terminal Emulator	2.19
	Setting IP Parameters	2.20
	Changing Community Names	2.20
2.10.3	Configuring Telnet Access	2.21
	Using snmplock Command to Limit SNMP Access from Outside Local Network to Logged-on Telnet Session	2.22
2.10.4	Configuring Optional Primary Base Mgmt Module	2.23
	Auto-negotiation for Base Mgmt Module Primary Status	2.23
2.10.5	Installing FocalPoint™ Software at Remote NMS	2.24
3.	OPERATION	3.1
3.1	Using Status LEDs	3.2
3.1.1	Media Conversion Center LED Indicators	3.2
3.1.2	Media Converter Slide-In-Module LED Indicators	3.2
3.2	Using PointSystem™ Web-Based Management	3.3
3.3	Using FocalPoint™ Software at Remote NMS	3.3

3.4	Using Management Command-line Interface (CLI)	.3.4
	At an Attached Terminal Interface	3.4
	At a Telnet Connection	3.5
3.4.1	Command-line Interface Commands	3.6
3.4.2	Command-line Interface Messages	3.12
3.4.3	Command-line Interface Trace Masks	3.36
4	MAINTENANCE	.4.1
4.1	Fault Isolation and Recovery	.4.2
4.1.1	At the Remote Network Management Station	4.2
4.1.2	At the Cabinet Front	4.4
4.2	Hardware Replacement Procedures	.4.6
4.2.1	Replacing Media Converter Slide-In-Module	4.6
4.2.2	Replacing Management Module	4.7
4.2.3	Replacing AC Power Supply Module	4.8
4.2.4	Replacing 48-VDC Power Supply Module	4.10
4.2.5	Replacing 48-VDC Power Supply Module Fuse	4.13
4.2.6	Replacing AC Power Supply Module Fuse	4.15
4.3	Firmware Upgrades	.4.16
Appendix A. PointSystem™ Technical Specifications		. . .A.1
Appendix B. Null Modem Cable Specifications		B.1
Appendix C. Introduction to SNMP in the CPSMC1900		.C.1
Appendix D. Displaying the CPSMC1900 MIB Tree		D.1
Appendix E. SNMP GLOSSARY		E.1
Appendix F. Power Consumption Data Sheet		F.1

Notes:

1. INTRODUCTION

The modular TRANSITION Networks *PointSystem™* CPSMC1900 series 19-Slot Network Media Conversion Center allows the network administrator to connect various copper and fiber network media, over protocols that include Ethernet™, Fast Ethernet™, DS3/E3, and OC-12, using various connectors on selectable TRANSITION Networks Media Converter Slide-in-Modules.

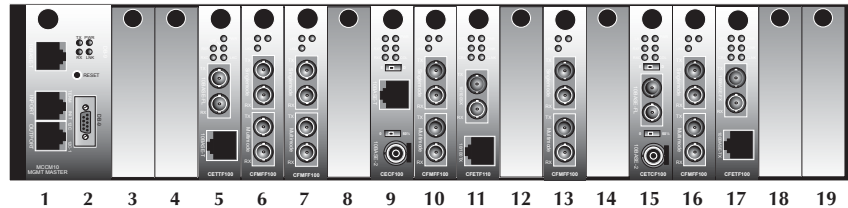
A *PointSystem™* Media Conversion Center with an installed Management Module can be monitored and managed at an attached terminal or terminal emulator or at a remote Telnet connection. An SNMP application such as TRANSITION Networks *FocalPoint™* network management software can be installed at a remote Network Management Station to monitor and manage up to eight (8) cascaded *PointSystem™* cabinets fully populated with installed Media Converter Slide-In-Modules.

This introduction to the 19-Slot Media Conversion Center provides:

1.1	The Media Conversion Center	1.2
1.1.1	AC Power Supply Module	1.2
1.1.2	Optional Redundant AC Power Supply Module	1.3
1.1.3	Optional 48-VDC Power Supply Module	1.3
1.1.4	Optional LED Slide-in-Module	1.4
1.1.5	Media Converter Slide-in-Modules	1.4
1.2	Optional Network Management	1.5
1.2.1	Management Module(s)	1.5
1.2.2	SNMP Agent in Base Management Module	1.7
1.2.3	Management Software at Command-line Interface	1.8
1.2.4	<i>PointSystem™</i> Network Security	1.10
1.2.5	<i>PointSystem™</i> Web-Based Management	1.12
1.2.6	<i>FocalPoint™</i> Software at Remote NMS	1.13

1.1 The Media Conversion Center

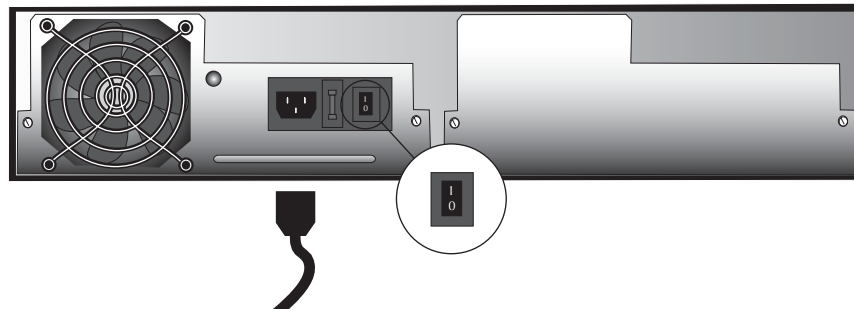
The modular TRANSITION Networks 19-Slot *PointSystem™ C* Media Conversion Center chassis provides installation space for up to nineteen (19) hot-swappable Media Converter Slide-in-Modules at the front and for one or two hot-swappable Power Supply Modules at the back.



1.1.1 AC Power Supply Module

An AC Power Supply Module, installed at the back of the Media Conversion Center before shipment, supplies power to the Media Conversion Center, to installed Media Converter Slide-in-Modules, and to the optional Management Module.

The following connector, switch, and indicator are located on the AC Power Module:

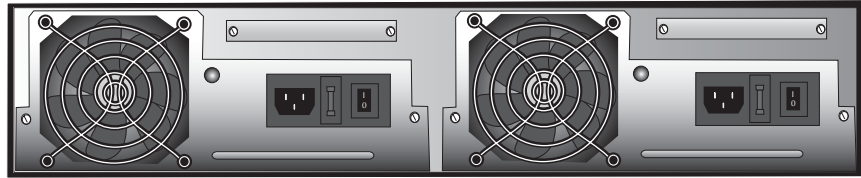


- An external power cord distributes power from an external AC outlet to an *AC power connector* on the AC Power Supply Module.
- An **ON/OFF switch**, set to **I**, allows the AC Power Supply Module to supply power to the Media Conversion Center and installed Slide-in-Modules.
- A *power LED indicator* is located on the AC Power Supply Module.

NOTE: An AC Power Supply Module *fuse* is installed in a fuse holder located between the AC power connector and the ON/OFF switch.

1.1.2 Optional Redundant AC Power Supply Module

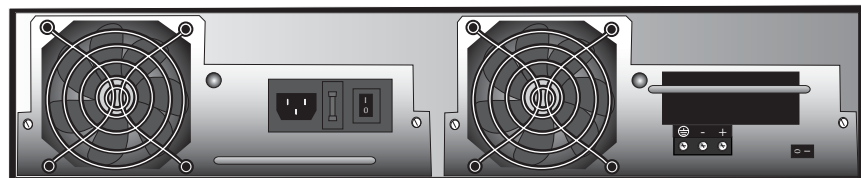
Space is available at the back of the Media Conversion Center for installing an optional redundant AC Power Supply Module.



NOTE: If two Power Supply Modules are to be installed in the Media Conversion Center, the network administrator can set Master/Slave switches installed on the Power Supply Modules to share power distribution automatically between the two Power Supply Modules OR to make one of the two Power Supply Modules *primary* and the other Power Supply Module *secondary*, but never both to secondary.

1.1.3 Optional 48-VDC Power Supply Module

Alternatively, an optional 48-VDC Power Supply Module can be installed



in either space or in both spaces.

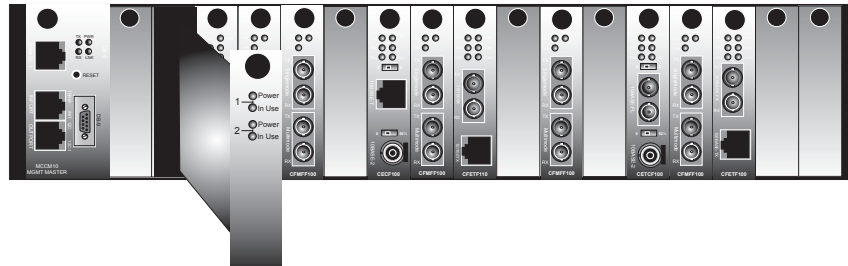
The following connectors, switch, and indicator are located on the 48-VDC Power Module:

- A three-position terminal block that distributes power from an external 48-VDC outlet to a *chassis ground connector*, to a *negative (-) connector*, and to a *positive (+) connector*
- An **ON/OFF** switch that, set to **I**, allows the 48-VDC Power Supply Module to supply power to the Media Conversion Center and to installed Slide-in-Modules
- An **LED power indicator**.

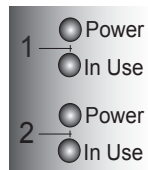
NOTE: A 48-VDC Power Supply Module *fuse* is installed on the 48-VDC Power Supply Module circuit board (located inside the CPSMC1900 series Media Conversion Center).

1.1.4 Optional LED Slide-in-Module

The optional LED Slide-in-Module, which can be installed in any slot at the front of the Media Conversion Center, allows the network administrator to determine at a glance which power supplies are installed and in use.



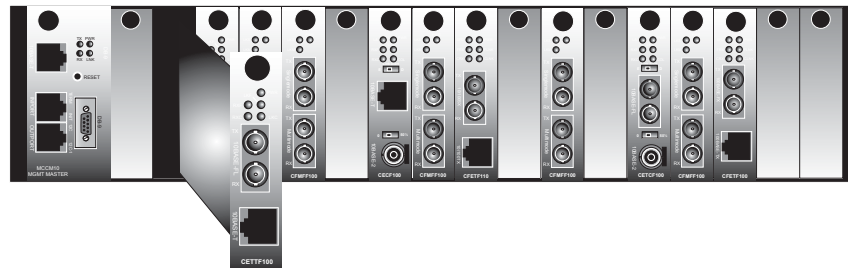
Power and **In Use** LED indicators for *each* installed Power Supply Module are provided on the installed LED Slide-in-Module.



NOTE: If an optional LED Slide-in-Module is installed in the 19-Slot Media Conversion Center, the LED Slide-in-Module initiates a self-test of the LEDs at Media Conversion Center power on. During the self-test, the LEDs are illuminated in marquee fashion. After the self-test, the LEDs indicate power supply operating conditions.

1.1.5 Media Converter Slide-in-Modules

NOTE: Media Converter Slide-in-Modules are all hot-swappable.



TRANSITION Networks Media Converter Slide-in-Modules, installed in slots at the front of the Media Conversion Center, allow the network administrator to connect various network media using connectors located on the Media Converter Slide-In-Modules.

NOTE: Refer to the documentation that comes with each Media Converter Slide-in-Module for cable, connector, and LED indicator information specific to that Media Converter Slide-in-Module.

1.2 Optional Network Management

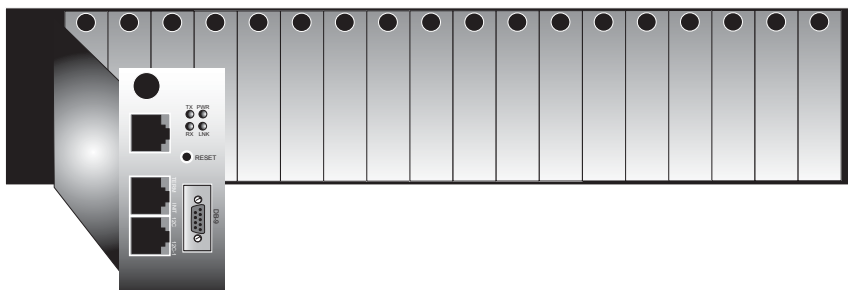
Optional *PointSystem™* network management is provided through Management Slide-In-Module(s) with embedded SNMP network management software.

1.2.1 Management Module(s)

Optional Management Module(s) that can be installed in the CPSMC1900 series Media Conversion Center include the Base Management Module and optional Expansion Management Module(s).

Base Management Module

The CPSMM-200 Base Management Module is installed in the CPSMC1900 series Media Conversion Center to enable network management.



The following connectors, indicators, and switch are located on the CPSMM-200 Base Management Module:

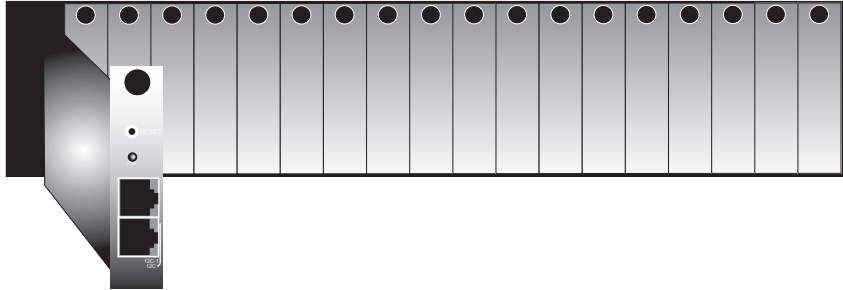
- A **DB-9 SERIAL-PORT**, through which the Base Management Module communicates with the command-line interface
- An **RJ-45 ETHERNET PORT**, through which the Base Management Module communicates through the Ethernet network with a remote Network Management Station (NMS) or a Telnet connection
- A set of non-Ethernet RJ-45 **CASCADE PORTS**, through which the Base Management Module is connected to other Management Module(s)
- A **RESET** switch, located on the Management Module, which resets the *Management Module ONLY*
- **POWER, LINK, RX (receive) and TX (transmit)** LED indicators.

NOTE: When two or more 19-Slot Network Media Conversion Centers are cascaded, a second Base Management Module can be configured as redundant.

NOTE: A non-cascading CPSMM-120 Base Management Module is available with identical connectors, indicators, and switch as on the CPSMM-200 except without non-Ethernet RJ-45 cascade ports.

Expansion Management Module

The CPSMM-210 Expansion Management Module is installed in the CPSMC1900 series Media Conversion Center to extend network management.



The following connectors and switch are located on the Expansion Management Module:

- A set of non-Ethernet RJ-45 **CASCADE PORTS**, through which the Expansion Management Module is connected to other Management Module(s)
- A **RESET** switch, located on the Management Module, which resets the *Management Module ONLY*

Cascade Option

The Management Module *Cascade option* allows the network administrator to connect up to eight (8) CPSMC1900 series Conversion Center PS units into one manageable stack, using a CPSMM-200 Base Management Module in the primary unit and an Expansion (or Base) Management Module in up to seven additional Conversion Center PS units to provide a

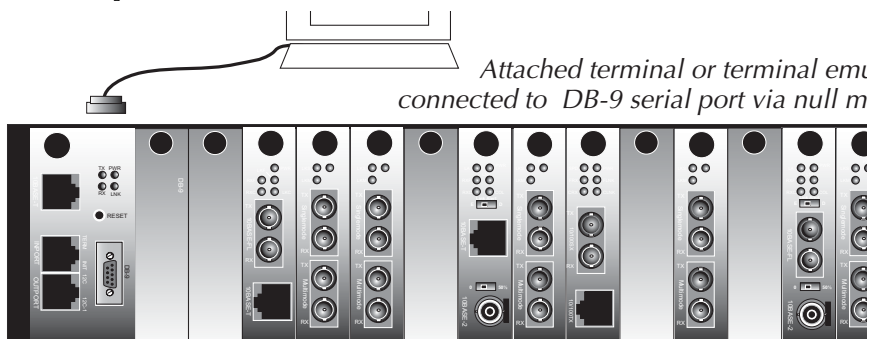


single management source for up to 135 conversion devices.

1.2.2 SNMP Agent in Base Management Module

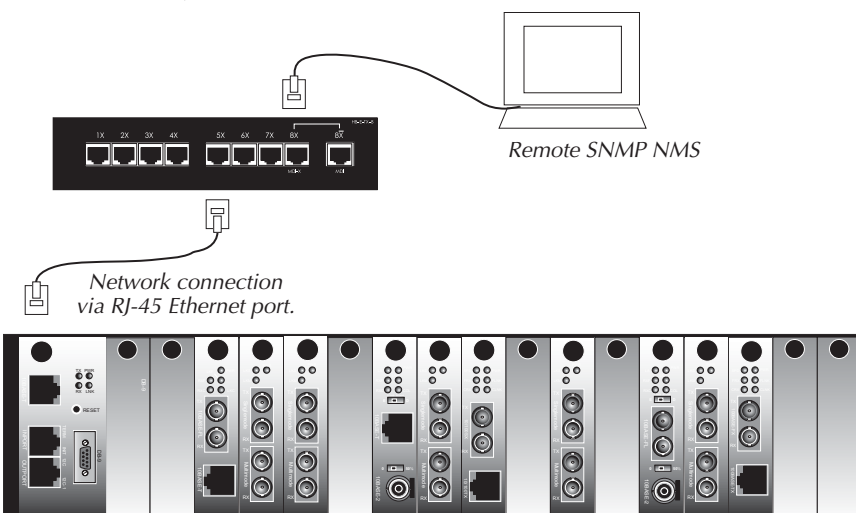
SNMP software installed in the Base Management Module can be accessed by the network administrator either through the serial-port DB-9 connector or through the network RJ-45 connector

Serial-port DB-9 Connection



The DB-9 serial-port permits the network administrator to configure and manage the CPSMC1900 series Media Conversion Center using a command-line interface at an attached terminal or terminal emulator.

Network RJ-45 Connection



The RJ-45 Ethernet connection permits the network administrator to manage the CPSMC1900 series Media Conversion Center using the FocalPoint™ graphical interface (or other SNMP application) at a remote network management station (NMS). The RJ-45 Ethernet connection also permits the network administrator to use a remote Telnet connection to the CPSMC1900 series Media Conversion Center.

The Base Management Module must be attached, through the RJ-45 Ethernet port, to a network that is accessible (via IP) from the computer at the remote location.

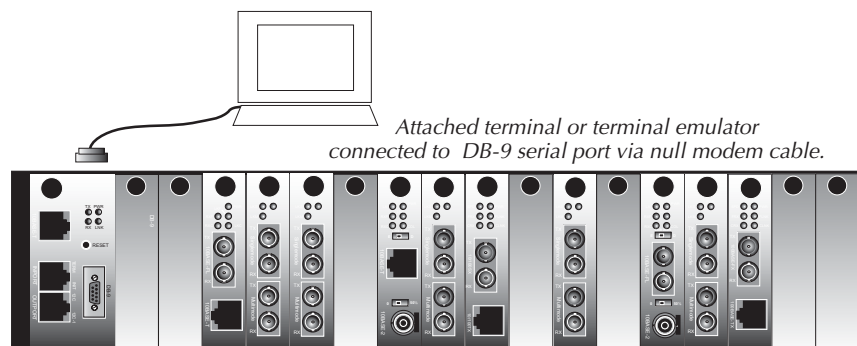
1.2.3 Management Software at Command-line Interface

The *PointSystem™* command-line interface (CLI) is accessible through the Management Module Serial Port and through the embedded Telnet Server. Analogous to a Unix shell prompt, the command-line interface allows all management data available via SNMP – including the CPSMC1900 status or any individual SNMP MIB variable supported by the Management Module – to be viewed and (where applicable) to be altered. The command-line interface also allows troubleshooting of the Management Module – and even of other stations on the network – using diagnostic commands and messages

NOTE: Aside from a few restrictions placed on Telnet access, the same interface is presented by these two methods.

CLI Access via Serial Port

To access the command-line interface (CLI) via the serial port, a serial terminal (or a computer with a terminal emulator) must be attached to the the Base Management Module DB-9 serial port via a null modem cable.

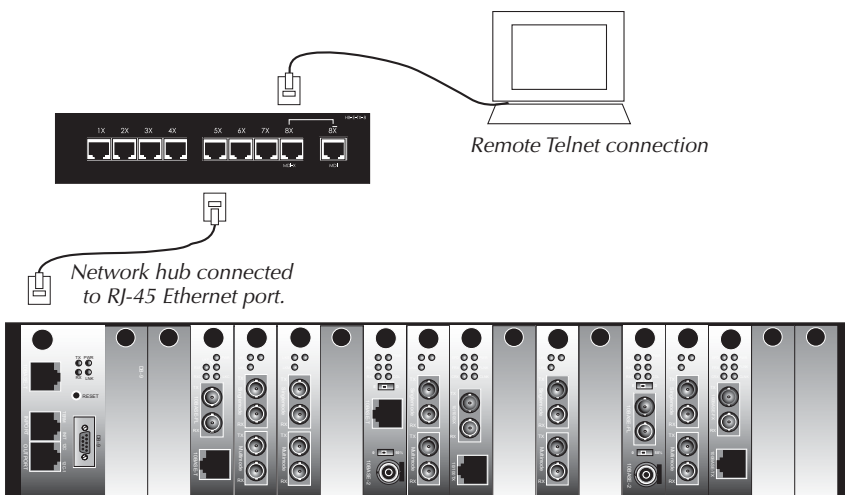


Serial-port command-line interface access is recommended or required in the following circumstances:

- When setting up or changing the IP configuration of the Management Module. Initial IP configuration is most commonly performed through the command-line interface via the serial-port. Subsequent IP configuration changes via Telnet are supported, but strongly discouraged.
- When optimizing performance, as during a troubleshooting session.
- When upgrading firmware, since firmware upgrade via the network is not supported.

CLI Access via Telnet

Telnet is useful when command-line interface access is desired from a physical location other than the wiring closet where the CPSMC1900 is installed. Any standard Telnet client (such as the one included with Windows 95) can be used from any location on the network.



To access the command-line interface via Telnet, the remote Telnet terminal must be attached to the Base Management Module's RJ-45 port via a network hub.

CAUTION: IP configuration changes take effect immediately when commands are received. Therefore, these changes should not be made via Telnet unless the user is confident that the implications of IP configuration changes are fully understood.

NOTE: Firmware upgrades cannot be performed via Telnet; serial-port command-line interface access is required.

1.2.4 PointSystem™ Network Security

TRANSITION Networks *PointSystem*™ network security is provided through password protection, remote Telnet access security, an SNMP lock command, and a console lock command.

Password Protection

The TRANSITION Networks *PointSystem*™ software provides two passwords that have the default values `private`, `public`:

`private` - used in three distinct roles:

SNMP read-write access (SNMP *PRIVATE* community name)

Telnet login access

CLI *superuser* mode access

`public` - for SNMP read-only access (SNMP *PUBLIC* community name)

PointSystem™ network security begins when the system administrator assigns unique, site-specific password values to replace the default values. (See Changing Community Names in 2.10.2 *Setting IP Parameters at Attached Terminal*.)

Remote Telnet Access Configuration

The TRANSITION Networks *PointSystem*™ Telnet server supports only a single connection at any given time. Additional concurrent connection attempts are rejected.

Since the authority granted to the Telnet command-line interface is not significantly more than that provided by the *PRIVATE* (most privileged) SNMP MIB view, the Telnet password is the same as the *PRIVATE* community name.

By default, the Telnet server accepts a connection from any client that provides the correct password. However, through the use of the command-line interface `set tntrip` and `set tntripmask` commands, the server can be configured to restrict access to a particular subnet, to restrict access to a particular station, or to disable Telnet altogether.

SNMPLOCK Command

The *PointSystem*™ **snmplock** command, entered at the *superuser* prompt in the format:

```
[SU] CPSMM100> SNMPLOCK=YES
```

allows the system administrator to cause the *PointSystem*™ agent to reject all SNMP traffic that originates outside of the local subnet, unless the source of that SNMP traffic also has an active, logged on Telnet session.

The **snmplock** command is intended to be used in conjunction with the **set tntrip** and **set tntripmask** commands, which permit the system administrator to cause the *PointSystem*™ Telnet server to reject traffic that does not originate from a specified, trusted subnet or station. (See 2.10.3 *Configuring Telnet Access*.)

When the **snmplock** command is in effect, the agent examines every incoming SNMP message. If the source IP for the command is on the local subnet, SNMP traffic is allowed. If the source IP for the SNMP traffic is NOT on the local subnet, the **snmplock** command requires the agent to look for an active Telnet session. If there is no active Telnet session, the SNMP traffic is denied. If there is an active Telnet session, the **snmplock** command requires the agent to compare the IP address of the source of the SNMP traffic with the IP address of the active, logged on Telnet session. If the IP addresses match, the SNMP traffic is allowed. If the IP addresses do not match, the SNMP traffic is denied.

Entering the *negative* **snmplock** command:

```
[SU] CPSMM100> SNMPLOCK=NO
```

again allows *PointSystem*™ SNMP traffic from any source IP, whether or not Telnet is active.

Console LOCK Command

The *PointSystem*™ **lock** command, entered in the format:

```
CPSMM100> lock
```

disables ALL command-line interface commands. When the *PointSystem*™ **lock** command is active, the “locked” state is indicated at the command-line prompt:

```
[locked] CPSMM100>
```

Any attempt to enter a command AT ANY TERMINAL when the command-line interface is locked results in a “Console is locked” response from the management agent.

Entering the command:

```
[locked] CPSMM100> SU=<case sensitive password>
```

overrides the **lock** command and unlocks the command-line interface.

1.2.5 PointSystem™ Web-Based Management

The TRANSITION Networks CPSMM100 Base Management Module contains an embedded HTTP (Web) server that allows the network administrator to use a standard Web Browser at a remote location for monitoring and configuring the *PointSystem™* Media Conversion Center.

Remote *PointSystem™* network management at a Web browser is through a set of screens that provide “views” of the network which bring the network administrator “to” the managed cabinets, then “closer” to the modules in a cabinet, and then even “closer” to module status conditions.

Detailed on-line help is provided as part of the *PointSystem™* Web-based network management.

Transition Networks
Point System Agent Summary
123.123.123/CPSMM100

Cabinet			
	Description	Model	P/N
view	1800	SMACF100LC	00001
view	1800	SMACF100/SNMP	00115
view	All Cabinets, All Modules		All

Group Control String: [apply](#)

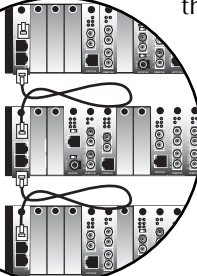
System uptime (d:h:m:s) : 00:15:30:10

[refresh](#)

[Help Topics](#)

After successful login to the primary CPSMM100 Base Management Module agent, all cabinets in the stack managed by that primary Base Management Module are listed in the **Agent Summary Display**.

ON-LINE HELP EXPLAINING NETWORK MANAGEMENT ARCHITECTURE AND METHODS IS AVAILABLE FROM THE AGENT SUMMARY DISPLAY.



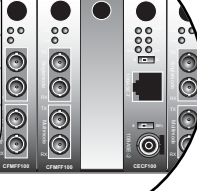
SMACF100 00257

	Cab	Slot	Device Summary
view	00257	1	SMACF100P - Switch Port Link=UP(1) Speed=100Mbps(1) Duplex=FDX(1)
view	00257	2	SMACF100P - Switch Port Link=UP(1) Speed=100Mbps(1) Duplex=FDX(1)
view	00257	3	SMACF100P - Switch Port Link=UP(1) Speed=100Mbps(1) Duplex=FDX(1)
view	00257	4	SMACF100P - Switch Port Link=UP(1) Speed=100Mbps(1) Duplex=FDX(1)
view	00257	5	SMACF100P - Switch Port Link=UP(1) Speed=100Mbps(1) Duplex=FDX(1)

[refresh](#) [agent summary](#)

Clicking on the **VIEW** icon next to a selected cabinet in the Agent Summary Display brings up the **Cabinet Summary Display**, with a list of all modules in the cabinet.

The list includes, for each module, module name, cabinet serial number and module slot location, with a quick summary describing the state of each listed module.



SMACF100-100 Switch Port (Cabinet=00257 Port=1)

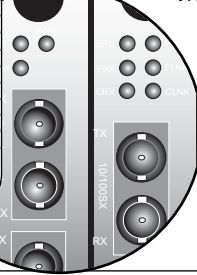
Port Parameter	Value
Group membership	
Config Match	N/A(3)
Media Connector	ST Singlemode Fiber (12)
Link Status	UP(1)
Interface Speed	100 Mbps (1)
Duplex	FDX(1)
Source Address	NO(2)
C - ange Detect Status	
Change Detect Config	DISABLED(2)
C - ritigent Address	80:00:0A:DE(1) 00
Interface Enabled	YES(1)

[save](#) [refresh](#) [device summary](#) [agent summary](#) [Troubleshooting Help](#)

Some changes may take 12 seconds or more to be reflected. Click the refresh button for an update.

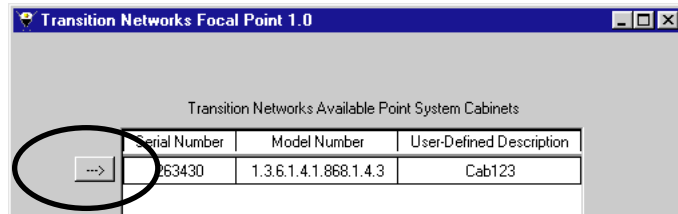
Clicking on the **VIEW** icon next to a listed module on the Cabinet Summary Display brings up a **Module Status Display**, which provides a list of parameters and associated parameter values for that module.

ON-LINE HELP, INCLUDING PARAMETER VALUE DESCRIPTIONS, IS AVAILABLE FROM THE MODULE STATUS DISPLAY.



1.2.6 FocalPoint™ Software at Remote NMS

FocalPoint™ software opens with a screen that lists the CPSMC series cabinets managed by the *PointSystem™* agent, with serial number, model number (MIB-II object ID), and user-defined description for each cabinet.



Clicking the **arrow** button at the left of a selected Conversion Center cabinet brings up a **Cabinet View** screen of that Conversion Center and of all installed Media Converter Slide-In-Cards.

Left-clicking on one of the the Slide-in-Module displays (but not the connector or LED) brings up the **Details** screen for that Slide-in-Module. Changing (and applying) fields on the **Details** screen changes the configuration for the Slide-in-Module. By grouping devices, the *PointSystem™* SNMP agent can be used to apply a single configuration change to a group of Slide-in-Modules of the same model.

Clicking the **Help** button or the **?** button **on any screen** brings up links to an integrated set of **HELP** screens that give detailed direction for using the *FocalPoint™* software and that CAN BE VIEWED AND PRINTED FROM ANY STANDARD HTML BROWSER.

Files displayed at the HELP screens are updated with the software to provide the most current and accurate reference for the FocalPoint™ software installed on the network.

2 INSTALLATION & SERVICE

Direction for installing the TRANSITION Networks *PointSystem™* Media Conversion Center is provided in the pages that follow.

2.1	Unpacking CPSMC1900 Equipment	2.2
2.2	Installing Optional Management Module in Media Conversion Center Chassis	2.3
2.3	Installing LED, Media Converter Slide-in-Module(s) in Media Conversion Center Chassis	2.5
2.4	Installing Optional Power Supply Module	2.6
	2.4.1 Setting Master/Slave-Management/Manual Switch	2.7
	2.4.2 Securing Power Supply Module to Chassis	2.9
2.5	Installing Optional Fan Module	2.10
2.6	Installing Media Conversion Center at Site	2.11
	2.6.1 Standard 19-Inch Rack Installation	2.11
	2.6.2 Table-Top Installation	2.12
2.7	Optionally Cascading Management Modules	2.13
2.8	Connecting Media Converter Slide-In-Modules to Network	2.14
2.9	Powering the Media Conversion Center	2.15
	2.9.1 Through the AC Power Supply Module	2.15
	2.9.2 Through the 48-VDC Power Supply Module	2.16
2.10	Optionally Configuring Network Management	2.17
	2.10.1 Network Security	2.17
	2.10.2 Setting IP Parameters at Attached Terminal	2.19
	2.10.3 Configuring Telnet Access	2.21
	2.10.4 Configuring Optional Primary Base Management Module	2.23
	2.10.5 Installing FocalPoint™ Software at Remote NMS	2.24

All Installation and service must be performed by qualified service personnel.

2.1 Unpacking CPSMC1900 Equipment

Use the following list to verify the shipment:

Item	Part Number
19-Slot Media Conversion Center	CPSMC1900-100
Power Cord	3344 (OR 3347, 3348, or 3349, depending upon country where installed)
LED Indicator Module	LPSLD-100 (optional)
Redundant AC Power Supply Module	CPSMP-200 (optional)
48-VDC Power Supply Module	CPSMP-210 (optional)
Redundant Fan Module	CPSFM-200 (optional)
2-slot Base Management Module	CPSMM-200 (optional)
1-slot Base Management Module	CPSMM-100 (optional)
FocalPoint™ Software Disk	FPS (provided with CPSMM-200)
Expansion Management Module	CPSMM-210 (optional)
Management Cascade Connector	6026 (optional)
User's Guide	33242
One or more selectable Media Converter Slide-in-Modules	Cnnnnxxxx

2.2 Installing Optional Management Module in Media Conversion Center Chassis

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Management Module in the 19-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Management Module.

NOTE: Install one (1) *Base Management Module* (CPSMM-200 or CPSMM-100) in the primary – or only – managed CPSMC1900 Conversion Center. Install one (1) *Base Management Module* or one (1) *Expansion Management Module* (CPSMM-210) in any secondary managed CPSMC1900 Conversion Center.

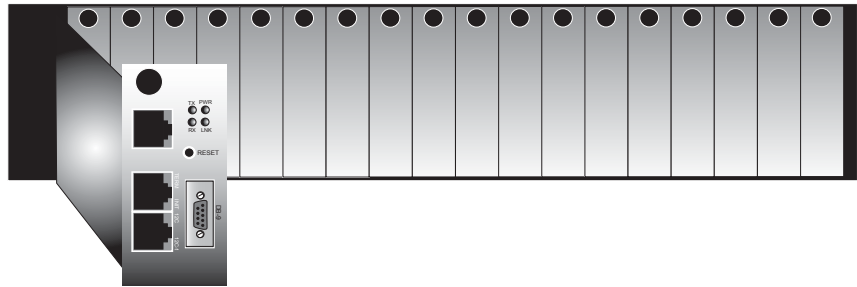
To install a Management Module in the CPSMC1900 chassis:

1. Carefully place CPSMC1900 on table or other flat, stable surface.

2 INSTALLATION & SERVICE

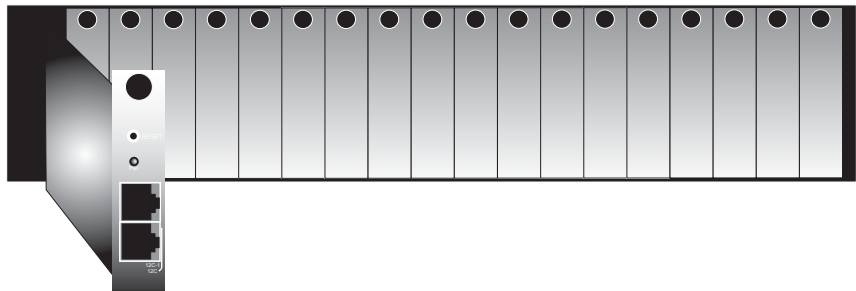
2. At CPSMC1900 front, locate Management Module installation slot on CPSMC1900 chassis.

NOTE: Though Management Module(s) can be installed in any Media Conversion Center slot, use of the leftmost installation slots for installing Management Module(s) is recommended in order to keep cascading cables separate from network cables installed on Media Converter Slide-In-Modules.



3. *CPSMM-200 2-Slot Base Management Module*
Remove two (2) Management Module protective plates from two (2) installation slots **at far left position** by removing one (1) screw that secures **each** protective plate to CPSMC1900 chassis.

OR



CPSMM-200 2-Slot Base Management Module OR CPSMM-210 Expansion Management Module

- Remove one (1) Management Module protective plate from one (1) installation slot **at far left position** by removing one (1) screw that secures protective plate to CPSMC1900 chassis.
4. Align Management Module with Media Conversion Center installation slot so that panel fastener screw is at top of Management Module.
5. Carefully slide Management Module into installation slot, aligning Management Module with installation guides.

NOTE: Ensure that Management Module is firmly seated against backplane.
6. Rotate attached panel fastener screw clockwise to secure Management Module to CPSMC1900 chassis.

2.3 Installing Selected LED, Media Converter Slide-in-Module(s) in Media Conversion Center Chassis

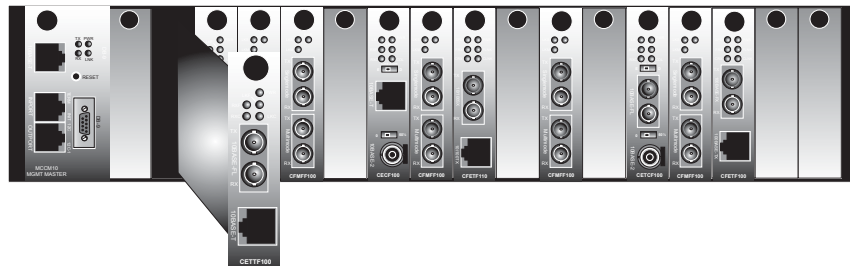
CAUTION: Before *FILLING* Media Conversion Center with Media Converter Slide-in-Modules, refer to the power consumption data for EACH model Media Converter Slide-in-Module (provided in User's Guide shipped with Media Converter Slide-in-Module) to determine optimum site configuration. Failure to observe this caution could result in diminishing system reliability.

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Media Converter Slide-in-Module(s) in the 19-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Media Converter Slide-in-Module(s).

To install the Media Converter Slide-in-Module in the CPSMC1900 19-Slot Media Conversion Center chassis:

1. Carefully place the CPSMC1900 19-Slot Media Conversion Center on table or other flat, stable surface.
2. Locate Media Converter Slide-in-Module installation slots at CPSMC1900 19-Slot Media Conversion Center front.

NOTE: Media Converter Slide-in-Modules can be installed in any installation slot, in any order.



3. Remove Media Converter Slide-in-Module protective plate from installation slot by removing one (1) screw that secures plate to front of CPSMC1900.
4. Align Media Converter Slide-in-Module with Media Conversion Center installation slot so that panel fastener screw is at top of Media Converter Slide-in-Module.
5. Carefully slide Media Converter Slide-in-Module into installation slot.
NOTE: Ensure that Media Converter Slide-in-Module is firmly seated against backplane.
6. Install Media Converter Slide-in-Module by carefully rotating attached panel fastener screw clockwise to secure Media Converter Slide-in-Module to CPSMC1900 chassis.
7. Repeat steps 3 through 6 for additional Media Converter Slide-in-Module(s).

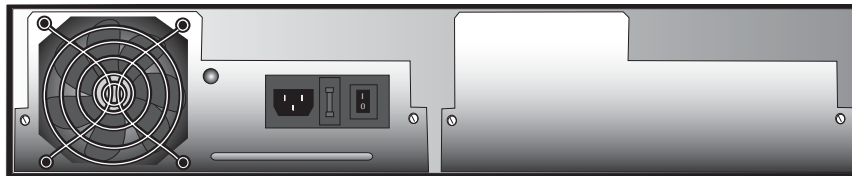
2 INSTALLATION & SERVICE

2.4 Installing Optional Power Supply Module

WARNING: DO NOT CONNECT POWER SUPPLY MODULE TO EXTERNAL POWER BEFORE INSTALLING IN MEDIA CONVERSION CENTER. FAILURE TO OBSERVE THIS CAUTION COULD RESULT IN EQUIPMENT DAMAGE AND/OR PERSONAL INJURY OR DEATH.

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when setting configuration switch and when installing Power Supply Module in Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module.

The standard CPSMC1900 is shipped, as shown, with one (1) AC Power Supply Module installed at the back of the CPSMC1900 cabinet and with a protective plate covering an installation slot intended for a second, optional Power Supply Module.

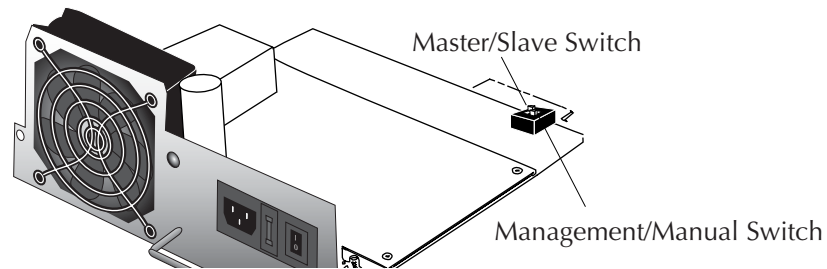


NOTE: Power Supply Modules can be “hot swapped”.

2 INSTALLATION & SERVICE

2.4.1 Setting Master/Slave-Management/Manual Switch

The CPSMC1900 Power Supply Module is shipped with a set of Master/Slave-Management/Module switches installed on the circuit board.



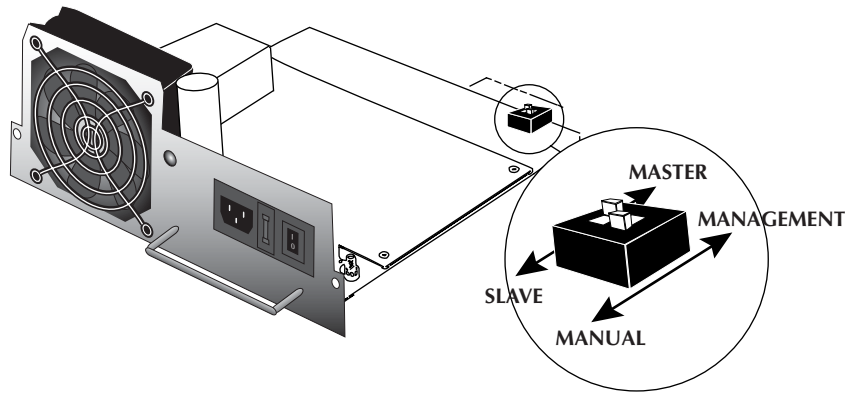
The **MASTER/SLAVE** switch allows the Power Supply Module to be configured as the primary (master) or as the secondary (slave) Power Supply Module. As primary (master), the Power Supply Module provides power to the chassis and all installed Slide-In-Cards, unless prevented from doing so due to external power source failure. As secondary (slave), the Power Supply Module waits in stand-by, ready to supply power to the chassis on primary (master) power source failure.

The **MANAGEMENT/MANUAL** switch allows TRANSITION Networks PointSystem™ software to control the primary (master) or secondary (slave) Power Supply Module setting AND TO OVER-RIDE THE PHYSICAL MASTER/SLAVE SWITCH SETTING ON THE POWER SUPPLY MODULE.

NOTE: When the MANAGEMENT/MANUAL switch is set to MANAGEMENT, the default MASTER/SLAVE configuration is primary (master) unless changed, at the software interface, to secondary (slave).

CAUTION: When installing two Power Supply Modules, AT LEAST ONE Power Supply Module MUST BE CONFIGURED AS PRIMARY (master). Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module(s).

CAUTION: In a 0-60° C environment, TWO POWER SUPPLIES MUST BE INSTALLED AND THE POWER SUPPLIES MUST BE CONFIGURED FOR LOAD-SHARING: one Power Supply Module must be configured as primary (master) and one Power Supply Module must be configured as secondary (slave). Failure to observe this caution could result in data transfer failure and/or damage to, and subsequent failure of, Power Supply Module(s).



NOTE: If both Power Supply Modules are configured as the primary (master) Power Supply Module, each Power Supply Module contributes a portion of the power to the chassis ("load sharing").

AC and DC Power Supply Modules are not intended to load share when used concurrently. When operating a Conversion Center with an AC Power Supply Module in one slot and a DC Power Supply Module in the other, both Supplies may not be set to 'Primary' (i.e., master).

1. Set MASTER/SLAVE switch, if necessary.
To configure the Power Supply Module as the primary (master) Power Supply Module, set MASTER/SLAVE switch to position labeled "MASTER". To configure the Power Supply Module as the secondary (slave) Power Supply Module, set MASTER/SLAVE switch to position labeled "SLAVE".
2. Set MANAGEMENT/MANUAL switch, if necessary.
To allow *PointSystem™* software to over-ride the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled "MANAGEMENT". To prevent *PointSystem™* software from over-riding the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled "MANUAL".

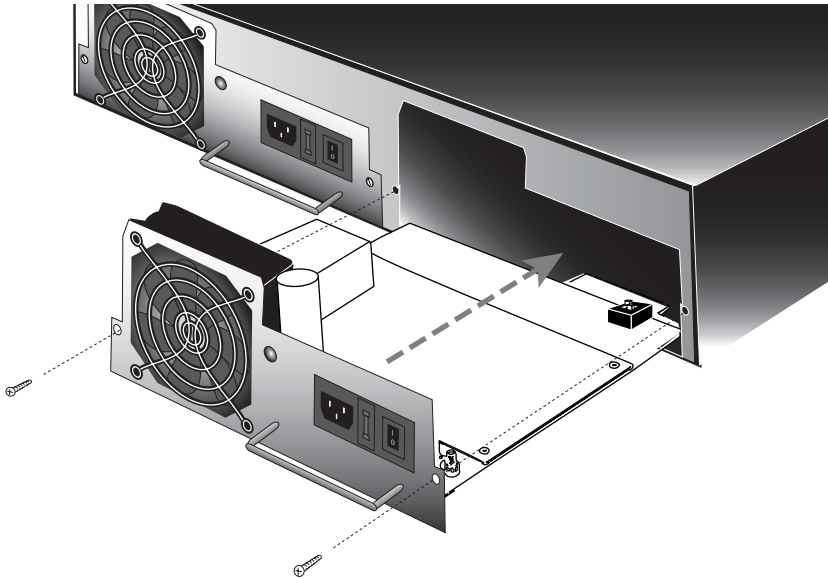
2.4.2 Securing Power Supply Module to Chassis

1. Locate protective plate at Power Supply Module installation slot on Media Conversion Center chassis back.



2. Remove Power Supply Module protective plate from installation slot by removing and retaining two (2) screws that secure protective plate to back of Media Conversion Center chassis.
3. Carefully slide Power Supply Module into Media Conversion Center installation slot, aligning Power Supply Module with installation guides.

NOTE: Ensure that Power Supply Module is firmly seated against chassis backplane. If the Power Supply Module does not fit flush against the frame, remove Power Supply Module from Media Conversion Center and repeat step 3 to ensure that Power Supply Module is aligned with installation guides.



4. Carefully install two (2) screws (retained in Step 2) through Power Supply Module into Media Conversion Center, rotating clockwise to secure.

2.5 Installing Optional Fan Module

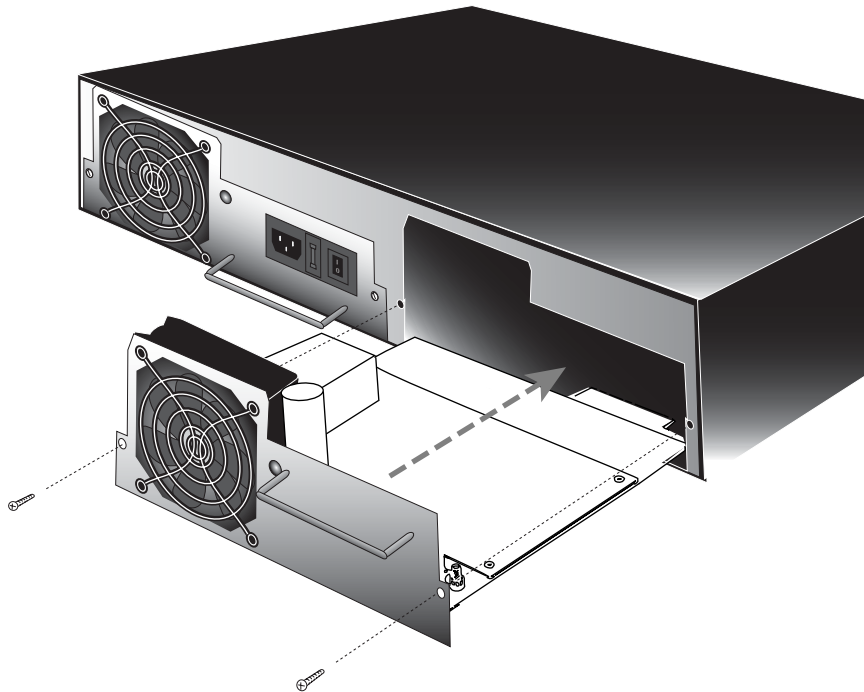
CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Fan Module in Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, Fan Module.

1. Locate protective plate at Power Supply Module/Fan Module installation slot on Media Conversion Center chassis back.



Remove protective plate from installation slot by removing and retaining two (2) screws that secure protective plate to back of Media Conversion Center chassis.

3. Carefully slide Fan Module into Media Conversion Center installation slot, aligning Fan Module with installation guides.



NOTE: Ensure that Fan Module is firmly seated against chassis backplane.

4. Carefully install two (2) retained screws through Fan Module into Media Conversion Center, rotating clockwise to secure.

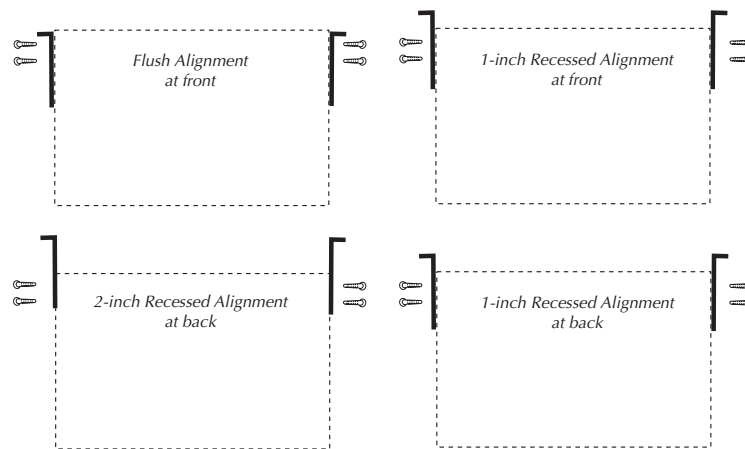
2.6 Installing Media Conversion Center at Site

The CPSMC1900 can be installed in a standard rack or on a table, shelf, or other stable surface.

2.6.1 Standard Rack Installation

The maximum recommended ambient temperature (Tmra) for the Conversion Center is 50C. (60C when using load sharing Power Supply Modules) If the Conversion Center is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the the rack environment may be greater than room ambient. Consideration should be given to installing the Conversion Center in an environment compatible with the Tmra.

Installation of the Conversion Center in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.



NOTE: The 19-Slot Media Conversion Center is designed so that the installation brackets can be installed to align the Media Conversion Center chassis either *flush* against the front or back edge of the rack or *recessed* from the front or back edge of the rack.

WARNING: SELECT MOUNTING BRACKET LOCATIONS ON THE MEDIA CONVERSION CENTER THAT WILL KEEP THE MEDIA CONVERSION CENTER BALANCED WHEN MOUNTED IN THE RACK. FAILURE TO OBSERVE THIS WARNING COULD ALLOW THE MEDIA CONVERSION CENTER TO FALL, RESULTING IN EQUIPMENT DAMAGE AND/OR POSSIBLE INJURY TO PERSONNEL.

Consideration should be given to the connection of the Conversion Center to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplates should be used when addressing this concern.

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

To install the 19-Slot Media Conversion Center in a standard rack:

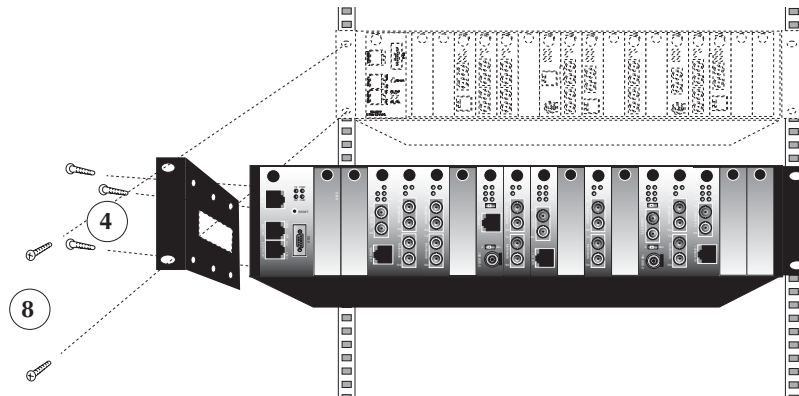
1. Determine preferred alignment of Media Conversion Center in rack.

NOTE: Installation bracket mounting screws are provided. Rackmount screws and clip nuts are NOT provided.

2. Locate six (6) installation bracket screws (*provided*) for each 19-Slot CPSMC1900 chassis to be installed.

WARNING: Mount Media Conversion Center chassis evenly and securely in rack. Failure to observe this warning could allow the Media Conversion Center to fall, resulting in equipment damage and/or possible injury to personnel.

3. Align universal mounting bracket in selected position against side of CPSMC1900 chassis so that chassis installation holes are visible through universal bracket installation holes.
4. Using Phillips screwdriver, install three (3) screws through mounting bracket into chassis installation holes on side of 19-Slot Media Conversion Center.
5. Repeat steps 3 and 4 for second mounting bracket.
6. Locate four (4) screws (*not provided*) and optional clip-nuts (*not provided*) for each 19-Slot Media Conversion Center to be installed.



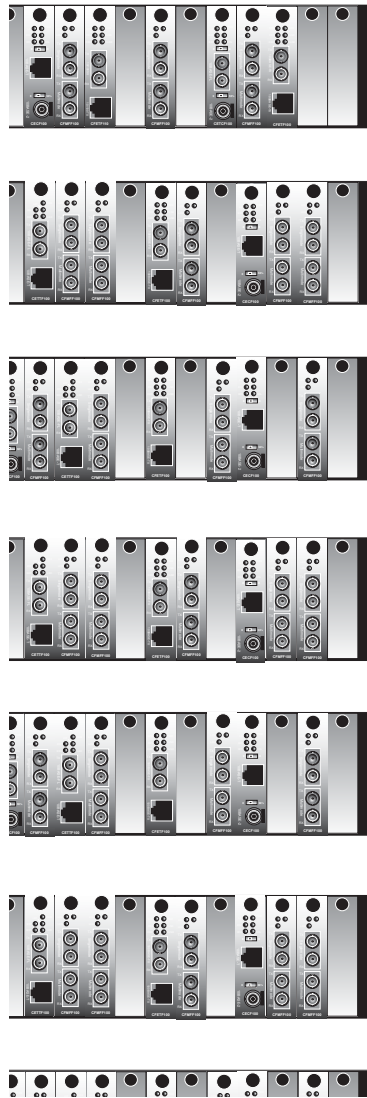
7. Carefully align 19-Slot Media Conversion Center at secure and level position between the site rack mounting rails.
8. Install two (2) screws through right bracket into right mounting rail and two (2) screws through left bracket into left mounting rail, using clip nuts to secure if necessary.

2.6.2 Table-Top Installation

The CPSMC1900 is shipped with installed rubber feet for optional installation on table or other flat, stable surface in well-ventilated area.

2.7 Optionally Cascading Management Modules

Cascade up to seven (7) CPSMC1900 Media Conversion Centers with installed **Expansion** Management Modules to one (1) CPSMC1900 Media Conversion Center with an installed **Base** Management Module.



Alternatively, install two **Base** Management Modules in a two-CPSMC1900 Media Conversion Center stack and cascade the Base Management Modules for redundant management.

To cascade two or more CPSMC1900 units:

1. Locate one (1) TRANSITION Networks CPSMC1900 Management Module cascade cable (with RJ-45 connectors installed at both ends) for each set of two (2) CPSMC1900 units to be cascaded.

NOTE: TRANSITION Networks CPSMC1900 Management Module cascade cables are one (1) meter long; ensure that CPSMC1900 units are installed within one (1) meter of each other.

2. Plug RJ-45 connector at one end of at CPSMC1900 Management Module cascade cable into *Base* Management Module RJ-45 connector at front of CPSMC1900 unit labeled **OUT**.
3. Plug RJ-45 connector at other end of at CPSMC1900 Management Module cascade cable into *Expansion* Management Module or second *Base* Management Module RJ-45 connector at front of *next* CPSMC1900 unit labeled **IN**.
4. Plug RJ-45 connector at one end of at CPSMC1900 Management Module cascade cable into *Expansion* Management Module or second *Base* Management Module RJ-45 connector at front of *that* CPSMC1900 unit labeled **OUT**.
5. Plug RJ-45 connector at other end of at CPSMC1900 Management Module cascade cable into *Expansion* Management Module RJ-45 connector at front of *next* CPSMC1900 unit labeled **IN**.
6. Repeat steps 4 and 5 until all CPSMC1900 units have been cascaded

2.8 Connecting Media Converter Slide-In-Modules to Network

CAUTION: Connect input/output network cables **ONLY** to Media Converter Slide-In-Module connectors within the same network protocol (such as Ethernet-to-Ethernet, Fast Ethernet-to-Fast Ethernet, ATM-to-ATM). Failure to observe this caution will cause data transfer to fail.

Refer to User's Guides that come with the Media Converter Slide-In-Modules for cabling specifications and direction.

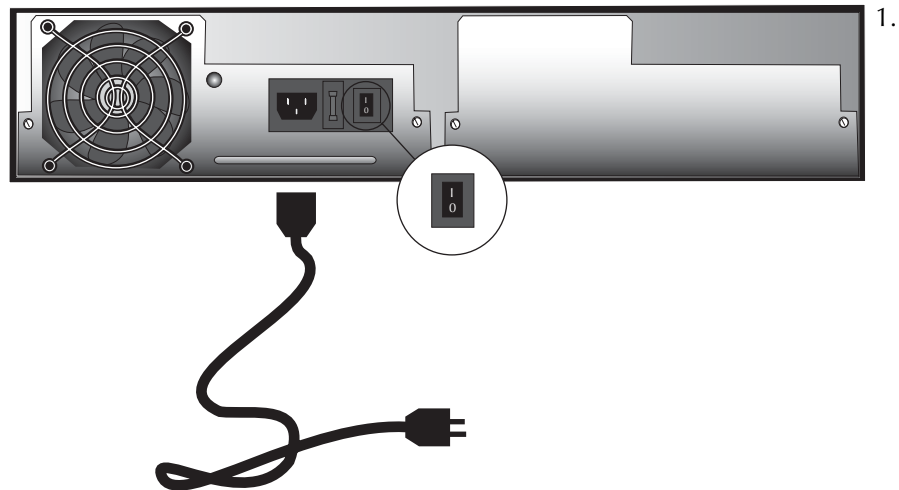
2.9 Powering the Media Conversion Center

The 19-Slot Media Conversion Center can be powered through the AC Power Supply Module and/or through the 48-VDC Power Supply Module.

NOTE: If an optional LED Slide-in-Module is installed in the 19-Slot Media Conversion Center, the LED Slide-in-Module initiates a self-test of the LEDs at Media Conversion Center power on. During the self-test, the LEDs are illuminated in marquee fashion. After the self-test, the LEDs indicate power supply operating conditions.

2.9.1 Through the AC Power Supply Module

To power the 19-Slot Media Conversion Center through the AC Power Supply Module:



1. Connect female end of power cord to power receptacle on Power Supply Module.
2. Plug male end of power cord into correct voltage AC rack or wall socket.
3. Set Power Supply Module power switch to I.
4. Verify that Media Conversion Center is powered by observing illuminated Power LED and fan operation.

2.9.2 Through the 48-VDC Power Supply Module

Read and follow all warning notices and instructions marked on the product or included in the manual

All installation and service must be performed by qualified service personnel.

This product is intended to be used in a restricted access location. Connect the product to a -48VDC SELV (Safety Extra Low Voltage) supply that is electrically isolated from the DC Source. The -48 VDC source is to be reliably connected to earth (ground). Equipment grounding is vital to ensure safe operation.

Prior to installation, use a voltmeter/ohmmeter to check the wiring for the presence of earth ground.

A readily accessible disconnect device as part of the building installation shall be incorporated into the fixed wiring. The disconnect device (a -48 VDC, 15 or 20A circuit breaker or switch) must be included in the ungrounded supply conductor. Overcurrent protection must be a 15 or 20A, -48 VDC fuse or circuit breaker.

CAUTION: Ensure that power source is NOT powered and that 48-VDC power ON/OFF switch is set to "O" when connecting to 48-VDC Power Supply Module. Failure to observe this caution could result in damage to, and subsequent failure of, 48-VDC Power Supply Module.

To power the 19-Slot Media Conversion Center through the 48-VDC Power Supply Module:

1. Connect +48-VDC terminal to Media Conversion Center terminal block control marked "+". Turn terminal screw clockwise to secure.
2. Connect -48-VDC terminal to Media Conversion Center terminal block control marked "-". Turn terminal screw clockwise to secure.
3. Connect ground terminal to Media Conversion Center terminal block control marked "chassis ground". Turn terminal screw clockwise to secure.
4. Set 48-VDC Power Supply Module power switch to I.
5. Verify that Media Conversion Center is powered by observing illuminated Power LED and fan operation.

2.10 Optionally Configuring Network Management

Configuring TRANSITION Networks *PointSystem*™ network management requires considering network security while setting IP parameters and configuring remote Telnet access.

2.10.1 Network Security

TRANSITION Networks *PointSystem*™ network security is provided through password protection, remote Telnet access security, an SNMP lock command, and a console lock command.

Password Protection

The TRANSITION Networks *PointSystem*™ software provides two passwords that have the default values `private` or `public`:

`private` - used in three distinct roles:

SNMP read-write access (SNMP *PRIVATE* community name)

Telnet login access

CLI *superuser* mode access

`public` - for SNMP read-only access (SNMP *PUBLIC* community name)

PointSystem™ network security begins when the system administrator assigns unique, site-specific password values to replace the default values. (See *Changing Community Names in 2.10.2 Setting IP Parameters at Attached Terminal.*)

Remote Telnet Access Configuration

The TRANSITION Networks *PointSystem*™ Telnet server supports only a single connection at any given time. Additional concurrent connection attempts are rejected.

By default, the Telnet server accepts a connection from any client that provides the correct password. However, through the use of the command-line interface `set tntrip` and `set tntripmask` commands, the server can be configured to restrict access to a particular subnet, to restrict access to a particular station, or to disable Telnet altogether.

NOTE: Since the authority granted to the Telnet command-line interface is not significantly more than that provided by the *PRIVATE* (most privileged) SNMP MIB view, the Telnet password is the same as the *PRIVATE* community name.

SNMPLOCK Command

The *PointSystem*™ **snmplock** command, entered at the *superuser* prompt in the format:

```
[SU] CPSMM100> SNMPLOCK=YES
```

allows the system administrator to cause the *PointSystem*™ agent to reject all SNMP traffic that originates outside of the local subnet, unless the source of that SNMP traffic also has an active, logged on Telnet session.

The **snmplock** command is intended to be used in conjunction with the **set tntrip** and **set tntripmask** commands, which permit the system administrator to cause the *PointSystem*™ Telnet server to reject traffic that does not originate from a specified, trusted subnet or station. (See 2.10.3 *Configuring Telnet Access*.)

When the **snmplock** command is in effect, the agent examines every incoming SNMP message. If the source IP for the command is on the local subnet, SNMP traffic is allowed. If the source IP for the SNMP traffic is NOT on the local subnet, the **snmplock** command requires the agent to look for an active Telnet session. If there is no active Telnet session, the SNMP traffic is denied. If there is an active Telnet session, the **snmplock** command requires the agent to compare the IP address of the source of the SNMP traffic with the IP address of the active, logged on Telnet session. If the IP addresses match, the SNMP traffic is allowed. If the IP addresses do not match, the SNMP traffic is denied.

Entering the *negative* **snmplock** command:

```
[SU] CPSMM100> SNMPLOCK=NO
```

again allows *PointSystem*™ SNMP traffic from any source IP, whether or not Telnet is active.

Console LOCK Command

The *PointSystem*™ **lock** command, entered in the format:

```
CPSMM100> lock
```

disables ALL command-line interface commands. When the *PointSystem*™ **lock** command is active, the “locked” state is indicated at the command-line prompt:

```
[locked] CPSMM100>
```

Any attempt to enter a command AT ANY TERMINAL when the command-line interface is locked results in a “Console is locked” response from the management agent.

Entering the command:

```
[locked] CPSMM100> SU=<case sensitive password>
```

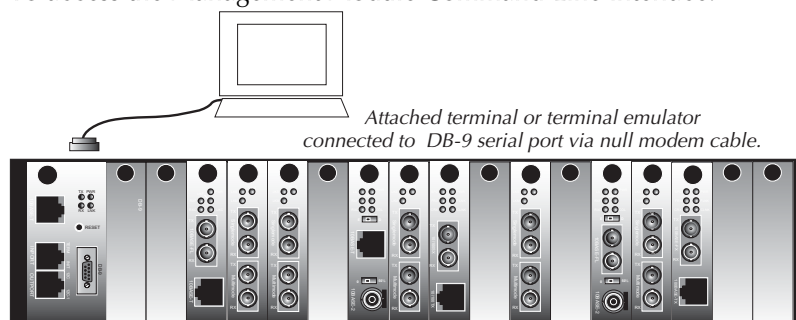
overrides the **lock** command and unlocks the command-line interface.

2.10.2 Setting IP Parameters at Attached Terminal

Attaching Terminal or Terminal Emulator

Network management can be configured ONLY if a Base Management Module is installed in the Media Conversion Center. (See 2.2 *Installing Optional Management Module in Media Conversion Center Chassis*.)

To access the Management Module Command-Line Interface:



1. Locate Base Management Module installed in Media Conversion Center.
2. Locate null modem DB-9 serial port cable with female DB-9 connector. (Refer to Appendix for null modem cable configuration).
3. Attach DB-9 serial port female cable connector to DB-9 serial port male connector on Base Management Module.
4. Attach other end of the DB-9 serial port cable to ASCII terminal or terminal emulator.

NOTE: By default, the 19-Slot Media Conversion Center uses the following serial port parameter values:

bits per second	9600*
stop bits	1
data bits	8
parity	NONE

* 38,400 bits per second also is supported. (See **bps** command in 3.3.1 *Command-line Interface Commands*.)

5. Using methods appropriate to the attached terminal, verify that the serial port parameters of the attached terminal match the 19-Slot Media Conversion Center port parameter values. If necessary, modify the attached terminal port parameter values.

After the terminal or terminal emulator has been attached to the Media Conversion Center and the Media Conversion Center has been powered (or reset), press **<return>** to bring up a command-line prompt at the attached terminal or terminal emulator:

```
CPSMM100> _
```

Setting IP Parameters

Set internet protocol (IP) network parameters through the attached terminal interface to allow Media Conversion Center SNMP or ICMP management

NOTE: The console prompt string is determined by the MIB variable ***cpsmm100.SysName.0***. The default value for this MIB variable is CPSMM100, as shown. Changing the value of ***cpsmm100.SysName.0*** changes the console prompt to the new value.

NOTE: When the community name is changed to a unique, site-specific value, that value replaces *private* in the **SU** command. (See below.)

To access the *superuser* command-line prompt for the first time, at the command line prompt, type and enter the command (using the *case-sensitive* password, *private*):

```
CPSMM100> SU=private
```

The superuser prompt comes up:

```
[SU] CPSMM100>
```

NOTE: When ANY of the following IP configuration commands is entered, the *PointSystem™* software validates all IP parameters, reporting problems until *all three* of the IP configuration commands have been entered successfully.

To set the IP, netmask, and gateway addresses, at the *superuser* command line prompt, type and enter (*in format: nnn.nnn.nnn.nnn*):

```
[SU] CPSMM100> SET IP=<IP address>
```

```
[SU] CPSMM100> SET NETMASK=<mask>
```

```
[SU] CPSMM100> SET GATEWAY=<gateway address>
```

To save the network configuration, at the *superuser* command line prompt, type and enter:

```
[SU] CPSMM100> SAVE
```

Changing Community Names

NOTE: Changing the *private community name* simultaneously changes the Telnet and superuser passwords.

To optionally set passwords by changing the default community names, at the *superuser* command line prompt, type and enter:

```
[SU] CPSMM100> SET PUBLIC=<public community name>
```

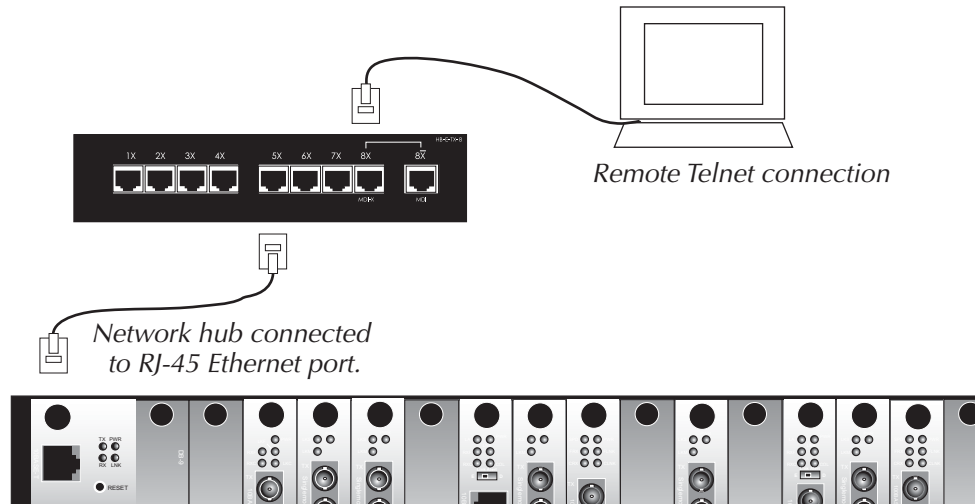
```
[SU] CPSMM100> SET PRIVATE=<private community name>
```

To save the network configuration, at the *superuser* command line prompt, type and enter:

```
[SU] CPSMM100> SAVE
```

2.10.3 Configuring Telnet Access

The Management Module command line interface can be accessed through a Telnet server on the Ethernet™ network. Any standard character-mode (preferred) or line-mode Telnet client can be used to gain access from any station not blocked by network security.



The Management Module's TCP uses the Telnet Remote IP address and the Telnet Remote IP address mask to validate incoming connection requests, allowing the network administrator to restrict Telnet access to one trusted subnet or even to a single, trusted location.

To permit Telnet connections from only a single location on the network (in this example, from IP address 206.5.22.11), type and enter:

```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> SET TNTRIP=206.5.22.11
[SU] CPSMM100> SET TNTRIPMASK=255.255.255.255
[SU] CPSMM100> SAVE
```

To permit Telnet connections from any station on the 206.5.22.0 subnet (if the subnet mask for this network is 255.255.255.0), type and enter:

```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> SET TNTRIP=206.5.22.0
[SU] CPSMM100> SET TNTRIPMASK=255.255.255.0
[SU] CPSMM100> SAVE
```

To permit Telnet connections from any station on any network, restore the default values:

```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> SET TNTRIP=0.0.0.0
[SU] CPSMM100> SET TNTRIPMASK=0.0.0.0
[SU] CPSMM100> SAVE
```

To disable the Telnet server, type and enter:

```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> SET TNTRIP=255.255.255.255
[SU] CPSMM100> SET TNTRIPMASK=255.255.255.255
[SU] CPSMM100> SAVE
```

NOTE: The `tntrip` and `tntripmask` may designate an authorized station or subnet anywhere on the Internet without regard for the Management Module's local IP and subnet mask. Also, the `tntripmask` need not correspond to any actual subnet.

Using `snmplock` Command to Limit SNMP Access from Outside Local Network to Logged-on Telnet Session

NOTE: The *PointSystem*™ `snmplock` command allows the system administrator to cause the *PointSystem*™ agent to reject all SNMP traffic that originates outside of the local subnet, unless the source of that SNMP traffic also has an active, logged-on Telnet session.

To use the `snmplock` command to restrict SNMP commands to the logged-on Telnet session, at the command line interface:

- Configure Telnet security (using `tntrip`, `tntripmask` commands) to restrict Telnet access to trusted locations.
- Enter the `snmplock` command:
[SU] CPSMM100> SNMPLock=YES
- Enter the save command to save the configuration to flash:
[SU] CPSMM100> SAVE

Then, at the remote NMS:

- Open a Telnet session to the agent.
- Launch *FocalPoint*™ (or other SNMP application) and make configuration changes to the agent.
- Close the Telnet session.

2.10.4 Configuring Optional Primary Base Management Module

When two Base Management Modules have been installed in a cascaded *PointSystem™* stack, the Base Management Modules auto-negotiate so that one *eligible* Base Management Module becomes *primary* and the other Base Management Modules become *stand-by*.

Management modules are *eligible* to become *primary* **only** if they are

- Base Management Modules AND
- assigned unique, valid IP configurations AND
- connected to the Ethernet network.

CAUTION: If no Base Management Modules are *eligible* to become primary, there can be NO primary Base Management Module. If there is no primary Base Management Module, though one or more cabinets may appear to the SNMP application to be installed on the network, no Slide-In-Modules or Power Supply Modules will appear to be installed in those cabinets. Thus, failure to observe this caution will result in the network administrator's inability to use SNMP to monitor or to manage Slide-In-Modules or Power Supply Modules.

The *primary* Base Management Module scans the bus looking for other modules, queries their status, provides changes to their configurations, and accepts SNMP and CLI set commands. The *stand-by* Base Management Modules listen as the primary Base Management Module scans the bus, record maps of the stack, and distribute information to modules, but cannot accept set commands.

To use the **WANTPRIMARY** command to weight a Base Management Module in the primary status auto-negotiation process, at the command-line interface ***of the terminal attached to the Base Management Module***, type and enter:

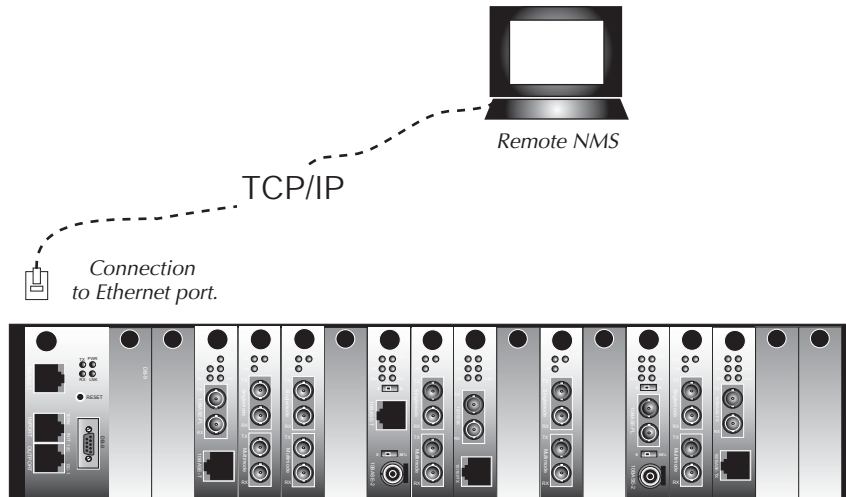
```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> WANTPRIMARY=YES
[SU] CPSMM100> SAVE
```

To return the Base Management Module to an unweighted state, at the command-line interface, type and enter:

```
CPSMM100> SU=<case sensitive password>
[SU] CPSMM100> WANTPRIMARY=NO
[SU] CPSMM100> SAVE
```

2.10.5 Installing FocalPoint™ Software at Remote NMS

To run the TRANSITION Networks *FocalPoint™* graphical interface at a remote network management station (NMS), first ensure that the *PointSystem™* Base Management Module is attached, through the 10BASE-T port, to a TCP/IP network that is accessible (via IP) from the network management station.



Then refer to the documentation that comes on the TRANSITION Networks *FocalPoint™* disk to find direction for installing the *FocalPoint™* network management software at the remote network management station.

Finally, refer to the extensive help files provided on the *FocalPoint™* disk for direction for using the *FocalPoint™* network management software.

3. OPERATION

Daily operation of the TRANSITION Networks *PointSystem*[™] CPSMC1900 Media Conversion Center requires no network administrator activity except the occasional monitoring of status LED indicators on the 19-Slot Media Conversion Center and on installed Media Converter Slide-In-Modules.

If the *PointSystem*[™] Media Conversion Center has an installed and configured Primary Management Module, the network administrator can manage the Media Conversion Center at an attached terminal or terminal emulator OR at a remote Telnet connection, using status and trace messages available at a command-line interface.

Additionally, a *PointSystem*[™] Media Conversion Center with an installed Primary Management Module can be managed using an SNMP application such as TRANSITION Networks *FocalPoint*[™] software at a remote Network Management Station (NMS) to monitor.

Or, the network administrator can manage a *PointSystem*[™] Media Conversion Center with an installed and configured Primary Management Module from the Web.

Direction is provided in the pages that follow:

3.1	Using Status LEDs	3.2
3.1.1	Media Conversion Center LED Indicators	3.2
3.1.2	Media Converter Slide-In-Module LED Indicators	3.2
3.2	Using PointSystem[™] Web-Based Management	3.3
3.3	Using FocalPoint[™] Software at Remote NMS	3.3
3.4	Using Management Command-Line Interface (CLI)	3.4
3.4.1	Command-Line Interface Commands	3.6
3.4.2	Command-Line Interface Messages	3.12
3.4.3	Command-Line Interface Trace Masks	3.36

3.1 Using Status LEDs

Status LEDs monitor *PointSystem™ Conversion Center™* operation.

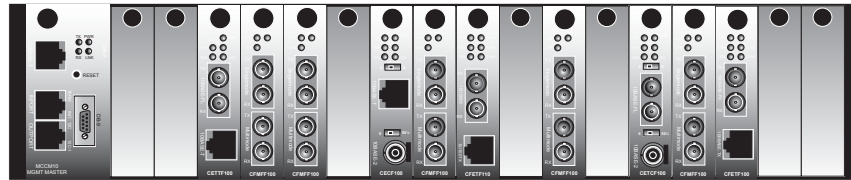
3.1.1 Media Conversion Center LED Indicators

Base Management Module Indicators

Power, Link, RX (receive) and TX (transmit) LED indicators located on the Base Management Module installed at the front of the primary Media Conversion Center indicate that the Media Conversion Center Management Module is powered, that a network link is established, and that the Management Module is either receiving or transmitting network data.

3.1.2 Media Converter Slide-In-Module LED Indicators

Refer to the TRANSITION Networks User's Guides that come with each Media Converter Slide-In-Module to interpret the LED indicators for the Media Converter Slide-In-Module(s).



3.2 Using PointSystem™ Web-Based Management

The information available at the LED displays on the physical CPSMC1900 cabinet also can be displayed at a standard Web Browser at a remote location because the CPSMM100 Base Management Module contains an embedded HTTP (Web) server.

To access the Transition Networks PointSystem™ Web interface, connect to the Base Management Module as to any other Web site, using appropriate Web Browser methods. (Connection typically is made by entering the IP address or DNS name of the PointSystem™ Base Management Module into the "Location" or "Go To" Web Browser box.)

When the Web connection is made, a login display comes up. At the login display, enter a case-sensitive password and then click on the login icon. If the password is valid, a display comes up with a list of the PointSystem™ Media Conversion Center cabinets to which the Base Management Module is attached.

Detailed on-line help is then available as part of the *PointSystem™* Web-based network management.

3.3 Using FocalPoint™ Software at Remote NMS

The information available at the LED displays on the physical CPSMC1900 cabinet also can be displayed at a *FocalPoint™* graphical interface at a remote network management station (NMS),

In addition, the *FocalPoint™* graphical interface allows remote management of the CPSMC1900 cabinet and installed slide-in modules.

To bring up the graphical display, click on the *FocalPoint™ icon* at the remote NMS in which the *FocalPoint™* graphical interface has been installed. Click the **Help** button OR the **?** button **on any screen** to bring up links to an integrated set of **HELP** screens that give detailed direction for using the *FocalPoint™* software and that CAN BE VIEWED AND PRINTED FROM ANY STANDARD HTML BROWSER:

3.4 Using Management Command-Line Interface (CLI)

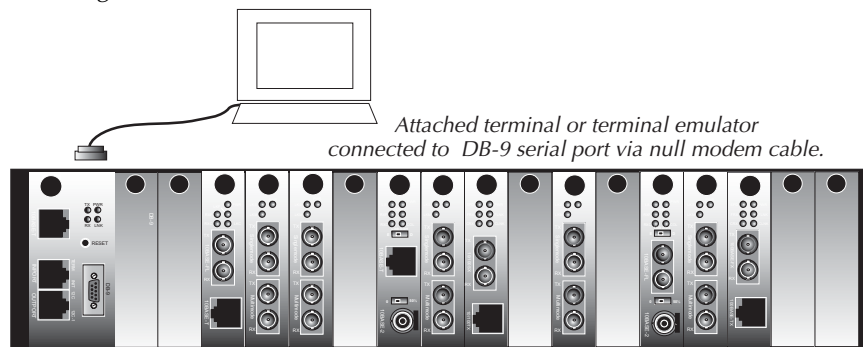
The Media Conversion Center Management Module command-line interface (CLI), analogous to a Unix shell and accessed from an attached terminal or from a remote Telnet location, permits the network administrator to display status messages and to display and to alter selected network settings.

At an Attached Terminal Interface

CAUTION: IP parameters should be set and/or modified *ONLY* at the attached terminal interface.

The Media Conversion Center command-line interface is accessible using a terminal or terminal emulator attached to the RS-232 serial port on the Media Conversion Center Management Module.

NOTE: The serial port cable is attached directly to a DTE device through a null modem cable. Refer to the Appendix for the null modem cable configuration.



1. Locate correct DB9 serial port cable with female DB9 connector.
2. Attach the DB9 serial port female cable connector to the male DB9 serial port connector on the Media Conversion Center.
3. Attach the other end of the DB9 serial port cable to an ASCII terminal or terminal emulator.

NOTE: By default, the 19-Slot Media Conversion Center uses the following serial port parameter values:

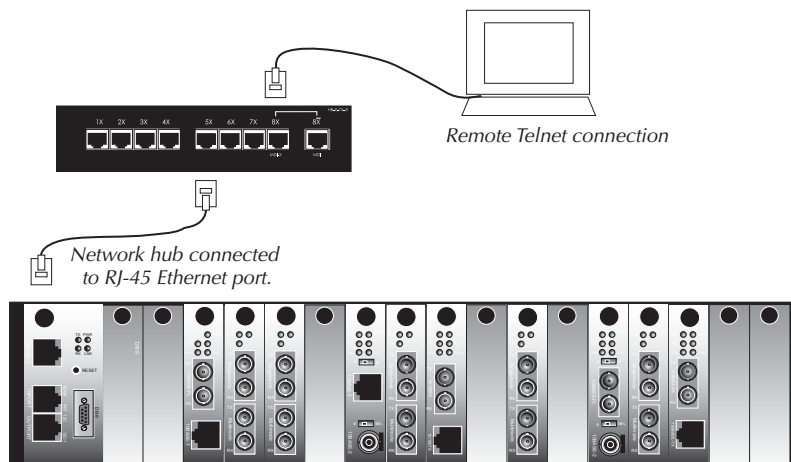
bits per second	9600*
stop bits	1
data bits	8
parity	NONE

* 38,400 bits per second also is supported. (See ***bps*** command in 3.4.1 Command-Line Interface Commands)

Using methods appropriate to the attached terminal, verify that the serial port parameters of the attached terminal match the 19-Slot Media Conversion Center port parameter values. If necessary, modify the attached terminal port parameter values.

At a Telnet Connection

The Media Conversion Center command-line interface is accessible using a remote Telnet connection to the Ethernet network which is attached to the RJ-45 port on the Media Conversion Center Management Module. Any standard character-mode (preferred) or line-mode Telnet client can be used to access the command line interface from any station not blocked by network security.



NOTE: The Telnet server supports only one session at a time. Additional concurrent connection attempts are refused.

When the client connects, a banner is displayed and the user is prompted to enter a password to gain access.

```
Transition Networks Telnet Server
System name: CPSMM100
Press CTRL-D to disconnect.
Enter password:
Remote console connected to nnn.nnn.nnn.nnn.
00:23:02:00 [su] CPSMM100>
```

The password is the same as the private community name. If an incorrect password is entered, the server immediately aborts the connection.

After the correct password is entered, the Telnet client is attached to the same console session available through the serial port. Users at the Telnet client and the serial terminal see the same messages and even see commands typed by the other user.

NOTE: Command-Line interface messages specifically related to Telnet or its underlying protocols are filtered out by the Telnet server to prevent storms of messages. Therefore, Telnet troubleshooting should always include inspection of the command-line messages at the serial-port interface.

Disconnect the Telnet client from the Management Module server by sending a CTRL-D, a Telnet EOF, or a Telnet ABORT command, by killing the Telnet client process, or by entering the LOGOFF command.

3.4.1 Command-Line Interface Commands

The Media Conversion Center Management Module command-line interface (CLI) is analogous to a UNIX shell.

“Brief” Internet Protocol (IP) Address Format

In most cases, a “brief” Internet Protocol (IP) address format is supported; if only the last octet of an IP address is specified, the other three octets are filled in automatically (based on the assumption that the new address is on the same subnet as the local IP address).

Using the “brief” IP address format, the following commands set the gateway IP to: 1.2.3.5

```
set ip=1.2.3.4
set netmask=255.255.255.0
set gateway=5
```

CAUTION: The behavior of this function may be non-intuitive when the subnet mask is not 255.255.255.0.

List of CLI Commands

Commands available at the command-line interface include:

? or h[elp]	<i>Displays the list of currently available commands. When in super-user mode (see the su= command) privileged commands are available.</i>
?command	<i>Displays help for console command.</i>
?=string	<i>Searches MIB for variable names or OIDs containing 'string'</i> <i>Example: "?=smmm05" searches for MIB variables containing "smmm05" which would yield all of the variables supported for the C/F-SM-MM-05 media converter.</i>
~	<i>If this character is typed at a command prompt, the previous command is executed again. (If you are connected via a line mode Telnet client, you will need to press ENTER.) Typing any other character (even if removed via the backspace key) clears the previous command so that it cannot be recalled using '~'.</i>
arp	<i>This command displays the current contents of the Address Resolution Protocol table. The left column contains the age of the entry in seconds, and the center and right columns respectively contain an Ethernet address and an IP address that are associated with each other.</i>
bps=9600/38400	<i>Sets the modem rate to either 9600 or 38,400 bits per second.</i>

clear or cls	<i>Clears the screen.</i>
get =(oid]	<i>Performs an SNMP GET operation on the local MIB database, using the given object ID (OID). The OID is expressed numerically or symbolically and, in either case, must be fully specified. If ‘=oid’ is omitted, the ending OID of the last successful GET/GETNEXT/SET command is used. Examples: “GET=1.3.6.1.2.1.1.3.0” Get current sysUptime value. “GET” Get sysUptime value again.</i>
getnext =(oid]	<i>Performs an SNMP GETNEXT operation on the local MIB database, using the given object ID (OID). GET/GETNEXT/SET command is used. This command behaves in a way similar to the GET command, except that the OID need not be fully specified, since it displays the data associated with the “next higher” OID, rather than an exact OID.</i>
gn	<i>A shorthand command equivalent to “GETNEXT”. No OID parameter is accepted, i.e. “GN=1.3.6” is not valid.</i>
lock	<i>Disables ALL command-line interface commands. When the PointSystem™ lock command is active, the “locked” state is indicated at the command-line prompt. Any attempt to enter a command AT ANY TERMINAL when the command-line interface is locked results in a “Console is locked” response from the management agent.</i>
logoff	<i>Closes the Telnet session. (Also activated by the Telnet commands: exit, logout, quit,</i>
memtest	<i>Executes a thorough DRAM diagnostic, as contrasted with the spot-check that is executed at system start</i>
ping [=nnn.nnn.nnn.nnn]	<i>Sends an ICMP ECHO message to the specified IP address. If no IP address is specified, the last valid IP address specified on a ‘ping’ command is used. The system transmits the ECHO message and acknowledges the command to the console. Note the sequence number and message ID contained in the console acknowledgement. These values are also displayed when incoming ECHO REPLY messages are reported, allowing the user to match ECHO REPLY messages with transmitted ECHO messages. The IP address specified with this command will be saved when a save command is issued.</i>
[reboot]	<i>Pressing the [escape] key five times in quick succession reboots the management software.</i>

Command-Line Interface - Commands

rping[=seconds]	Toggles repetitive ping. The rping command transmits an ICMP echo message once per second until the rping command is issued again. Prior to issuing this command, a destination IP address must be supplied by issuing a ping command with a legal IP destination. The state of this command will be saved when a save command is issued. If an interval (in seconds) is specified, that interval is used instead of the default (1 second). Specifying an interval of 0 seconds cancels rping.
save	This command saves many of the parameters set by the other commands in this section to FLASH memory. Once saved, the settings persist through rebooting and power cycling. Saved settings can be overwritten at any time by issuing another save command.
set=oid,type,value	Performs an SNMP SET operation on the local MIB database, using the given OID, type and value. The OID is expressed numerically and must be fully specified. If an asterisk (*) is specified in the place of the OID, the ending OID of the last successful GET/GETNEXT/SET command is used. Type = data type associated with variable being set, using: "INTEGER", "STRING", "IP". Value = the data to be assigned to the SNMP MIB variable.
set gateway=nnn.nnn.nnn.nnn	Sets the gateway IP address, the address of the station to which the Management Module transmits all datagrams with destinations that are not on the local subnet. This setting will be lost at the next reboot or power cycle unless the save command is issued.
set ip=nnn.nnn.nnn.nnn	Sets the IP address of this Management Module. This setting will be lost at the next reboot or power cycle unless the save command is issued.
set netmask=nnn.nnn.nnn.nnn	Sets the subnet mask that the Management Module will use when transmitting datagrams. This setting will be lost at the next reboot or power cycle unless the save command is issued.
set private=privatecommunityname	Sets the private community name. This community name must be used in all SNMP SET requests transmitted to the management card, and is also the password used to initiate super-user mode at the command line interface (see the su= command) and also is the Telnet password. The default private community name is "private". This setting will be lost at the next reboot or power cycle unless the save command is issued.

3 OPERATION

set public=*public community name* Sets the public community name. This community name must be used in all SNMP GET and GETNEXT requests transmitted to the management card. The default public community name is "public". This setting will be lost at the next reboot or power cycle unless the save command is issued.

set tntrip=*nnn.nnn.nnn.nnn* Sets the TELNET Remote IP address.

set tntripmask=*nnn.nnn.nnn.nnn* Sets the TELNET Remote IP mask.

Together, these two commands allow the network administrator to control which stations are permitted to access the Management Module via TELNET. See 3.12.

NOTE: Super User mode must be in effect. Changes made during TELNET session take effect at logout.

set trapmgr=*nnn.nnn.nnn.nnn* Sets the IP address to which all SNMP Traps will be sent. If the address is 0.0.0.0, NO traps are sent. A value of 255.255.255.255 results in traps being broadcast to ALL stations. Super User mode must be in effect.

show Displays configuration and status information.

snmplock=*yes/no* Allows the network administrator to cause the PointSystem™ agent to reject all SNMP traffic that originates outside of the local subnet, unless the source of that SNMP traffic also has an active, logged on Telnet session.

sql=*length* This command allows the maximum Length (in bytes) of the Serial output Queue to be set. This queue holds text data waiting to be displayed on the console. When a large value is used, the chances of display data being dropped due to high backlog are reduced, but system performance can be seriously degraded under peak loads. Values that are too small may cause erratic display behavior, such as incomplete displays. Range: 200 to 65335. Default: 2000.

stat Displays a summary of the conversion devices and power supplies that are installed in the Media Conversion Center.

su=*private community name* Initiates super user mode. In this mode, privileged operations (such as save) are available.

su Terminates super user mode.

Command-Line Interface - Commands

tcpstat	Intended for use under the direction of TRANSITION Networks Technical Support to show the current status of TCP connections. Shows if a Telnet session is active and the IP address of any client. If a session is inactive, the state is indicated by "s=2", and the remote IP address and mask, indicated by the "r=rip/ripmask(port)" entry, are those configured using the "SET TNTRIP" and "SET TNTRIPMASK" commands. If a session is active, the state of the connection is indicated by "s=5" and the remote IP address shown is that of the currently connected client.
tm=mask	Sets trace mask to the hexadecimal value specified. Enter: ?tm for a list of available trace bits. CAUTION: Using this command may seriously degrade system performance.: The mask is always entered and displayed in hex, and is the combination of all of the currently selected traces - each represented by a single bit. The default mask is 8101h - local SNMP trap condition + checksum + ICMP errors
trappoll=n	Sets the time interval at which slide-in cards are polled for trap conditions such as "link down". The value specified is the number of 1/10 second time ticks between polls, in decimal. Default is 10 (1 second). NOTE: Super User mode must be in effect.
wantprimary=yes/no	Allows the network administrator to weight a Base Management Module in the primary status auto-negotiation process. (Entered at the command-line interface of the terminal attached to the affected Base Management Module.):
xr	Initiates firmware update into management card. This process allows updated software to be loaded into the Management Module. To update the software, 1) obtain the newest compatible version from TRANSITION Networks, 2) attach the management card's serial port to a terminal emulator that supports the XMODEM/CRC (256 byte blocks) protocol, 3) issue the XR command, and 4) initiate a "Send" or "Upload" command from the terminal emulator to send the new software to the Management Module. CAUTION: If the 'write' phase is interrupted or fails for any reason, the CPSMC1900

3 OPERATION

Management Module will be damaged and will require servicing from TRANSITION Networks. Using a battery-backed uninterruptible power supply is highly recommended.

CAUTION: This software cannot check to make sure that the software that is downloading is compatible with the hardware into which the software is loaded. Incorrect software changes may damage the Management Module necessitating factory service. If you have any doubts, contact TRANSITION Networks for assistance before starting

CAUTION: Firmware update may cause all saved settings to be lost.

3.4.2 Command-Line Interface Messages

Messages that might be displayed at the command-line interface are listed in alphabetical order. Each item in the list includes an explanation of the probable source of the message and, where indicated, provides a suggested corrective action in response to the message.

ARP: no response from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to an expected packet that failed to arrive at the Ethernet interface. It indicates that the Management Module has abandoned (due to timeout) an attempt to determine the Ethernet address of the station it was asked to communicate with. Possible causes: 1) The destination station is down or does not exist 2) the subnet mask is set incorrectly 3) Ethernet communications have been disrupted. This message is printed only when the appropriate traces are enabled via the "TM=mask" command.

ARP: REQUEST from *nnn.nnn.nnn.nnn/nn nn nn nn nn nn* for *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. It indicates that another station (whose IP and Ethernet addresses are indicated at the beginning of the message) is attempting to determine the Ethernet address of the Management Module via Address Resolution Protocol (ARP). The Management Module answers each ARP request with a message containing the requested information. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

ARP: REQUEST sent for *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface or in response to a console command. It indicates that the Management Module has transmitted an Address Resolution Protocol (ARP) packet in an attempt to determine the Ethernet address of the station whose IP address is noted at the end of the message. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

ARP: RESPONSE from: *nnn.nnn.nnn.nnn=nn nn nn nn nn nn* to: *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the Management Module has (via ARP) successfully determined the Ethernet address of the station whose IP address is noted at the beginning of the message. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

[BNRY=0]

This unsolicited message indicates a latent software defect or a hardware failure in the Ethernet controller. Call TRANSITION Networks for assistance.

Command only available in super-user mode. Enter 'SU='

This message is a response to a console command. You have entered a privileged command without first entering super-user mode. The privileged command is rejected. Enter "SU=" followed by the private community name, and then re-enter the command that caused the error.

Community name changed. Use SAVE command to make permanent.

This message is a response to a console command. The public or private community name was changed via the "PUBLIC=new-public" or "PRIVATE=new-private" commands. This message warns you that the changes made will be lost the next time the Management Module is reset, rebooted, or power cycled - unless they are saved in FLASH memory as suggested.

[console overflow]

This unsolicited message indicates that console output messages were lost due to overflow. The preferred method for correcting this situation is to reduce the amount of console output by using the "TM=" command to suppress messages. In the small number of cases where this is not sufficient or not applicable, the user can increase the buffer space available for queued output by using the "SQL=" command. This should be attempted with caution.

NOTE: Use of the "SQL=" command only increases the system's capacity to handle larger momentary peaks in console output; it does NOT increase the system's sustained console printing ability. In fact, due to the resources consumed by a high SQL allocation, the system's overall performance (including the sustained printing rate) may be substantially reduced. SQL is always reset to its default value when the system is reset.

[Count]

This is an advanced debug message that should be displayed only when debug traces have been enabled at the advice of TRANSITION Networks technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that one of the Ethernet controller's internal counters has overflowed. This message can be ignored or disabled via the "TM=mask" command.

CPU ADDRESS ERROR, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn

This unsolicited message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

<D>

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An incoming Ethernet packet was discarded because the receive queue was full, i.e. Ethernet packets are arriving more quickly than they can be processed. This may occur occasionally (during periods of peak network load) without indicating a problem. However, if the message cannot be explained by heavy Ethernet traffic and it repeats more than a few times a minute or system operation is impaired, call TRANSITION Networks for assistance. To eliminate these messages, use the "TM=mask" command to disable the traces.

DMA ADDRESS ERROR, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn

This unsolicited message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

DOWNLOAD: Format of downloaded file is incorrect. Firmware update aborted. DOWNLOAD: Please reset the Management Module.

This message indicates that the signature at the end of the transferred file was incorrect, i.e. the file you are attempting to transfer is not a valid firmware module. The update process is aborted and the management module is halted as a precaution. Note that if you obtained new firmware in .ZIP format, you must unzip it before transferring it to the management module.

Command-Line Interface - Messages

DOWNLOAD: Invalid internal checksum. x=nnn, c=nnn Firmware update aborted.

DOWNLOAD: Please reset the Management Module.

The checksum calculated after the end of the XMODEM transfer did not compare correctly. Note that this probably does not indicate a problem with the XMODEM transfer into the management module. Instead, this probably indicates that the source firmware file you are attempting to transfer is corrupted. The update process is aborted and the management module is halted as a precaution.

DOWNLOAD: Press the ESC key to continue

This message is a response to the "xr" console command. This message is printed periodically after a firmware update attempt, under the assumption that the terminal emulator will fail to display console traffic it thinks is part of the XMODEM transfer. Waiting for an ESC before printing any final messages reduces somewhat the chances that your terminal emulator will mask them. When you see this message, press ESC and the XMODEM termination message(s) will be displayed.

DOWNLOAD: XMODEM/CRC receive error: tttt

DOWNLOAD: Rebooting

This message is a response to the "XR" console command. The XMODEM /CRC transfer failed. The last XMODEM/CRC error is displayed. Values for **tttt** include:

"Timeout" - Timeout waiting for data

"Serial" - low level serial transmission error

"Protocol" - Unimplemented protocol, i.e. not XMODEM/CRC

"EOT" - Received End Of Text from remote

"Canceled" - Received CANCEL from remote

"Retries - EOT" - too many retries on EOT

"Retries - C" - too many retries on C.

"Retries - Receive" - too many retries on receive. This is the code that will be displayed if the Management Module never sees any attempt by the terminal emulator to start the transfer.

"Unexpected packet number" - packet received out of sequence.

"Last Packet resent" - duplicate packet discarded

"Bad CRC" - Data was corrupted in transit

"Not start of packet" - Expected SOT, STX or EOT

"Not ACK" - Expected ACK or NAK

"Received max # bytes" - received packet too big

To resolve XMODEM receive problems, check the following:

1) Is serial cable configured correctly, in good condition, and plugged in firmly?

NOTE: Issuing console commands and receiving appropriate responses indicates null-modem cable is wired correctly.

2) Is XMODEM/CRC protocol used for the transfer? This protocol uses a 16 bit CRC with 128 byte data blocks. Neither original XMODEM (8 bit checksums with 128 byte data blocks) nor XMODEM-1K (16 bit CRCs with 1024 byte data blocks) is supported. NOTE: Many terminal emulator implementations use XMODEM/CRC but describe it as "XMODEM."

3) Is the transmitting station fast enough? Place the code on a local hard disk and use that copy as the source for your XMODEM/CRC transfer.

DOWNLOAD: XMODEM/CRC receive success, *nnn* bytes!

DOWNLOAD: FLASH 'WRITE' phase beginning. DO NOT INTERRUPT!

This message is a response to the "xr" console command. The XMODEM/CRC transfer was successful. This message is your "last chance" to abort the firmware update operation. When this message is displayed, you have approximately seven seconds left before the write begins (assuming that your terminal emulator displays it immediately when it is transmitted). If the write is interrupted, the Management Module will be damaged.

ETH: Can't transmit. Reason=*nn tttt*

This unsolicited message is printed periodically as applications attempt to transmit Ethernet packets. All outgoing Ethernet traffic has been halted. One or more reason code bits (*nn*) are expanded to text (*tttt*).

"Software incompatible with hardware." Contact TRANSITION Networks technical support for assistance.

"Invalid IP/Netmask/Gateway configuration." Local IP address, subnet mask, and/or default gateway are improperly configured. Further explanation of the configuration error will be provided by other messages. For more information, see console commands "SET IP=*nnn.nnn.nnn.nnn*".

"Software Shutdown." Reset the Management Module. Contact TRANSITION Networks if the message persists.

"Link Down." Indicates a problem with the link to the Management Module.

"Hardware initialization failed." Verify that the Management Module is properly connected to an active 10Base-T Ethernet port. Power cycle the Management Module. If message persists, contact TRANSITION Networks technical support.

ETH: ERROR, This version of the driver cannot run on this hardware revision.

The Ethernet driver has determined that it is definitely incompatible with the hardware version it is attempting to run on. The ethernet driver is disabled. A software update is required to correct this problem. Contact TRANSITION Networks technical support.

ERROR: Invalid configuration checksum. All saved values ignored.

This is a system startup message. The Management Module has disabled its network interface as a safety precaution. The user should (at a minimum) enter an IP address (via the "SET IP=*ip*" command), a subnet mask (via the "SET NETMASK=*mask*" command), and a gateway address (via the "SET GATEWAY=*ip*" command), then enter the "SAVE" command. This message is normal after a firmware upgrade but, at other times, may indicate a latent software defect or a hardware failure. If the message persists or recurs after performing the suggested corrective action, call TRANSITION Networks for assistance.

ETH: Invalid frame type, len=0x*nnnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the protocol type field of an incoming Ethernet II frame is not recognized, or the frame is not a valid Ethernet II frame. This usually indicates the presence on the local Ethernet segment of broadcast traffic that the Management Module is not programmed to interpret. The only supported types are ARP and IP over Ethernet II. This message is printed only when the appropriate traces are enabled via the "TM=*mask*" command. This message does not indicate an error condition. No corrective action is required.

Command-Line Interface - Messages

ETH: Link is now [UP | DOWN]

This unsolicited message indicates that the state of the management module's link to the ethernet hub has changed. While 'link=UP' is an excellent indication that communication with the hub has been achieved, it is not an **absolute** guarantee. If link is up and stations on the network are active, yet the ARP table remains empty, begin to suspect that something is wrong with hub or cable.

ETH: Unsupported protocol 0xnnnn

See “ETH: Invalid frame type, len=0xnnnn”

ETH: Warning, unknown model identifier.

This is a system startup message. The Ethernet driver does not recognize the model identifier of the hardware it is attempting to run on. This probably indicates that the software is older than the hardware. The driver attempts to continue, but correct operation cannot be guaranteed. A software update is required to eliminate this message. Contact TRANSITION Networks technical support.

ETHERNET INITIALIZATION FAILED

This unsolicited message is displayed when an unusual hardware or software condition is detected. An attempt to initialize the Ethernet controller failed. Power cycle the Management Module. If the message persists, call TRANSITION Networks for assistance.

ETHERNET RESET FAILED

See “ETHERNET INITIALIZATION FAILED”

FLASH: Erase verify failed. nnnn invalid words.

This message is a response to a console command. This message indicates a hardware failure or latent software defect. Retry the operation. If the message persists, call TRANSITION Networks for assistance.

FLASH: Function not implemented.

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: Illegal return code.

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: Illegal target address range

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: ROM starting address is not on sector boundary.

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: Saving configuration, please wait up to one minute...

This message is a response to a console command. The Management Module is saving its configuration to flash (i.e. non-volatile) memory. If this operation is interrupted, the saved configuration will be invalid and the Management Module will be unable to access the network (e.g. it will be unable to respond to SNMP requests) until IP parameters are re-entered. In this case, media converters installed in the Media Conversion Center continue to operate normally. The primary purpose of the SAVE operation is to make sure that the appropriate network parameters (i.e. IP address, subnet mask, and gateway address) are automatically available should the Management Module be rebooted for any reason, though other parameters are saved as well.

FLASH: Source data does not fit in specified target range.

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: This version of the software does not support flash.

This message is a response to a console command. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

FLASH: Write complete.

This message is a response to a console command. An attempt to save data or code in FLASH (i.e. non-volatile) memory was successful.

FLASH: Write verify failed. *nnnn* invalid words.

This message is a response to a console command. This message indicates a hardware failure or latent software defect. Retry the operation. If the message persists, call TRANSITION Networks for assistance.

GENERAL ILLEGAL INSTRUCTION, SP=*nnnnnnnn* PC=*nnnnnnnn* SR=*nnnnnnnn*

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

[h=*nnnn*]

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. The Ethernet interface has failed. Call TRANSITION Networks for assistance.

**ICMP: DESTINATION UNREACHABLE message received from *nnn.nnn.nnn.nnn* (ignored)
ICMP: code=*tttt***

Where *tttt* is "NETWORK UNREACHABLE," "HOST UNREACHABLE," "PROTOCOL UNREACHABLE," "PORT UNREACHABLE," "FRAGMENTATION REQUIRED and DF SET," or "SOURCE ROUTE FAILED."

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A gateway or host has determined that a datagram sent by the Management Module cannot be delivered. Frequently, this is due to an invalid IP address or a router, firewall or host configuration problem. A numeric value for *tttt* indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

Command-Line Interface - Messages

ICMP: ECHO message received from *nnn.nnn.nnn.nnn*, id=*nnn* seq=*nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The named station is PINGing the Management Module. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: ECHO REPLY message received from *nnn.nnn.nnn.nnn*, id=*nnn* seq=*nnn*

Unsolicited message displayed in response to a packet that arrived at the Ethernet interface. A PING response was received. Note the identification and sequence numbers; similar numbers are displayed when the PING packet is transmitted. The values can be used to match transmissions with responses. See RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: INFORMATION REQUEST message received from *nnn.nnn.nnn.nnn* (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This probably means that another host is attempting to find out what network it is on. The incoming ICMP message is ignored, since the Management Module does not support the INFORMATION service. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: INFORMATION REPLY message received from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message should never be displayed, since the Management Module does not support the INFORMATION service. If the message persists, call TRANSITION Networks for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: invalid checksum, perhaps from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming ICMP message was invalid. This is usually due to the corruption of the datagram in transit. Note that the source address displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

ICMP: PARAMETER PROBLEM message received from *nnn.nnn.nnn.nnn* (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A datagram sent by the Management Module was discarded by the named host. This message indicates that a message was corrupted in transit, or that an incompatibility exists between the networking code in the Management Module and the networking code in the named station. If the message persists, call TRANSITION Networks for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: REDIRECT message received from *nnn.nnn.nnn.nnn* (ignored)

ICMP: code=*tttt* recommended gateway=*nnn.nnn.nnn.nnn*

Where *tttt* is “REDIRECT for NETWORK”, “REDIRECT for HOST”, or “REDIRECT for NETWORK and TOS”.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is sent by the ‘from ip’ gateway when multiple gateways are attached to the local subnet and the Management Module is using a less-than-ideal gateway to reach its destination host. Since the Management Module does not support the use of multiple gateways, the only guaranteed way to eliminate this message is to place the Management Module on a subnet with only one gateway. If this is not possible, the Management Module’s gateway address can be changed to match the recommended gateway - though this will probably result in more redirect messages from the new gateway. Note that if the gateway that sent the redirect message conforms to standards, it will forward the data transmitted by the Management Module to the correct gateway and the messages can simply be disabled or ignored. A numeric value for *tttt* indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: ROUTER ADVERTISEMENT message received from *nnn.nnn.nnn.nnn* (ignored)

ICMP: ROUTER SOLICITATION message received from *nnn.nnn.nnn.nnn* (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. These messages are displayed when ICMP Router Discovery messages are received. The Management Module does not support ICMP Router Discovery. The incoming ICMP messages are ignored. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 1256, ICMP Router Discovery Messages, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: SOURCE QUENCH message received from *nnn.nnn.nnn.nnn* (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Due to congestion, the named gateway or host is requesting that the Management Module slow the flow of datagrams. Since the Management Module almost never transmits unsolicited datagrams, this message is ignored. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

Command-Line Interface - Messages

ICMP: TIME EXCEEDED message received from *nnn.nnn.nnn.nnn* (ignored)

ICMP: code=tttt

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A datagram sent by the Management Module was not delivered due to timeout in transit.

When tttt is "TTL EXPIRED IN TRANSIT" this means that a gateway saw a Time-To-Live value of zero - probably indicating a routing loop or other network configuration error. Note that the Management Module assigns the maximum legal Time-To-Live value to each outgoing datagram.

When tttt is "REASSEMBLY TIMER EXPIRED" this means that datagram fragment reassembly timed out at the destination host, which is caused by 1) the loss of one or more of the fragments in transit, 2) a short reassembly timer at the destination host, or 3) an extremely slow network path.

A numeric value for tttt indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: TIMESTAMP message received from *nnn.nnn.nnn.nnn* (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The incoming ICMP message is ignored, since the Management Module does not support the TIMESTAMP service. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: TIMESTAMP REPLY message received from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message should never be displayed, since the Management Module does not support the TIMESTAMP service. If the message persists, call TRANSITION Networks for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: UNKNOWN TYPE 0xnn message received from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that an unknown ICMP message was received. Some network vendors transmit proprietary types and codes in ICMP messages. If the message persists, contact the vendor of the transmitting station for assistance, or contact TRANSITION Networks if you are reasonably sure the type is not proprietary. If system operation is not impaired, then no corrective action is required. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For information on possible new ICMP messages see the RFC collection, available via anonymous FTP from NIC.DDN.MIL.

Illegal character

This message is a response to a console command. A non-printable character (outside the range 20h to 7Eh) was seen in a community name entered from the console.

illegal length. 1-30 characters required.

This message is a response to a console command. Re-enter the console command, making sure that the community name entered falls within the given bounds. No white space is permitted anywhere in the command.

Illegal register read *nnnn nnnn nnnn*

Illegal register write *nnnn nnnn nnnn*

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

ILLEGAL SLOT INSTRUCTION, SP=*nnnnnnnn* PC=*nnnnnnnn* SR=*nnnnnnnn*

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

Incorrect password.

This message is a response to a console command. The correct "SU=password" password is the same as the private community name. The default is "private". If you have forgotten your private community name and are unable to retrieve it from your Network Management Station, call TRANSITION Networks for assistance.

***** Invalid IP address: *tttt***

This message is a response to a console command. An invalid local or gateway IP address was entered. An IP address must be entered as "a.b.c.d" where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the address 0.0.0.0 is entered for a local IP address (but not for a gateway address). It is not possible to use this address as a local or gateway IP address.

***** Invalid subnet mask: *tttt***

This message is a response to a console command. An invalid subnet mask was entered. The subnet mask must be entered as "a.b.c.d" where a, b, c, and d are decimal integers from 0 to 255. A further requirement for the subnet mask is that it consist of a single region of all '1' bits at the most-significant end and a single region of '0' bits at the least significant end (i.e. no '1' bit is permitted to the right of any '0' bit, and no '0' bit is permitted to the left of any '1' bit). No white space is permitted anywhere in the command.

Invalid password, access denied.

See "TELNET: An invalid login attempt was rejected..."

IP: Incoming datagrams with invalid checksums are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a datagram with an invalid IP checksum is received, and for every 256 such datagrams after that. Unless this message is displayed frequently, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

IP: Incoming datagram fragment from *nnn.nnn.nnn.nnn* discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the transmitting station (identified by its IP address) or a gateway along the way has split the message into fragments. The Management Module does not support IP fragmentation or reassembly, so the traffic is discarded. Fragmentation is usually triggered by a message that is too large to fit into the Maximum Transmission Unit (MTU) of one of the networks it must pass through. Large messages are created when a network management application attempts to perform a GET or a SET operation on a large number of variables at once; try splitting such requests up. Another possible cause is that the message passed through a non-Ethernet network with a small MTU. If possible, route the traffic around this network. This message is printed only when the appropriate traces are enabled via the "TM=mask" command.

IP: Incoming fragmented datagrams are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a IP datagram fragment is received, and for every 256 datagram fragments after that. See also "IP: Incoming datagram fragment from *nnn.nnn.nnn.nnn* discarded"

IP: Invalid IP checksum, possibly from *nnn.nnn.nnn.nnn* IP: checksum calculated=*nnnn* transmitted=*nnnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming IP datagram was invalid. This is usually due to the corruption of the datagram in transit. Note that the address displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. Unless this message is displayed frequently or system operation is impaired, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

IP: Unsupported protocol 0xnn from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The datagram is addressed to a protocol not supported by the Management Module. For example, if another station attempts to exchange EGP messages with the Management Module, this message will be displayed since the Management Module does not support EGP. Supported protocols: ICMP, UDP, TCP. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

IP: Warning, no default gateway address specified. dest=*nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The Management Module has been asked to transmit a packet to a destination that is not on the same subnet as its own IP address, but no gateway address has been configured (via the "SET GATEWAY=ip" command). The Management Module will attempt to locate the destination station on the local Ethernet segment without using a gateway - this process almost always fails. This message is printed when any traces (including the default traces) are enabled via the "TM=mask" command.

Local IP=*nnn.nnn.nnn.nnn* Gateway IP=*nnn.nnn.nnn.nnn* Subnet mask=*nnn.nnn.nnn.nnn*

This message is a response to a console command. The network configuration settings currently in use are shown. These settings are not necessarily compatible or correct, and have not necessarily been saved. Once the settings have been proven to work, they should be saved to non-volatile memory via the "SAVE" command.

CPSMC1900>

This is a prompt that indicates that the Management Module's command line interface is ready for another non-privileged command. To enter privileged commands, first enter the "SU=private" command.

NOTE: The console prompt string is determined by the MIB variable *mib2.system.sysName*. The default value for this MIB variable is CPSMC1900, as shown here. Changing the value of *mib2.system.sysName* will change the appearance of the console prompt.

Memory test failed at *nnnnnnnn*

This is a system startup message. The DRAM test encountered an error. Power cycle the system. If the message persists, contact TRANSITION Networks for assistance.

New trace mask = *nnnnnnnn*

This message is a response to a console command. The trace mask was successfully changed. For more information, see the description of the "TM=mask" command.

NON-MASKABLE INTERRUPT, SP=*nnnnnnnn* PC=*nnnnnnnn* SR=*nnnnnnnn*

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

[Overflow nn]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that the controller's receive buffer has overflowed. The Ethernet controller is reset as a precaution. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the "TM=mask" command.

Command-Line Interface - Messages

PING: Traces of ICMP error indications have been enabled.

Trace mask: old=nnnnnnnn new=nnnnnnnn. Type ?TM for more information.

This message is displayed in response to a PING or RPING command entered from the console. This console message indicates that console tracing of incoming ICMP error indications (e.g. "Destination Unreachable") was previously suppressed, but has now been enabled. (It is recommended that this trace never be disabled.) These traces are automatically re-enabled when a PING or RPING command is entered because when a PING operation fails, the reason for the failure can often be detected and reported back to the originating station (via an Internet Control Message Protocol (ICMP) message) by another station (such as a router), and the suppression of this information can be a significant hindrance to network troubleshooting. **PING: invalid destination IP address.**

This message is a response to a console command. This indicates a syntax error in the entry of an IP address. Enter "PING=a.b.c.d" where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the IP address 0.0.0.0 is entered. It is not possible to ping this invalid address.

PING: pinging nnn.nnn.nnn.nnn, id=nnn seq=nnn

This message is a response to a console command. This message is displayed each time a ICMP ECHO packet is transmitted, i.e. once when a "PING" command is entered, and multiple times if the "RPING" command is entered. Note the identification and sequence numbers. They may be compared with those displayed when responses are received.

[Reset]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that the controller has entered the reset state or that the controller's receive buffer has overflowed. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the "TM=mask" command.

[rr:no buffer nnnn]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. An incoming Ethernet packet was discarded due to lack of memory. The number is the byte count of the packet, in hex. If this trace message occurs frequently, it indicates one of the following: 1) Excessive network traffic directed at the Management Module: 1a) Simultaneous SNMP requests from a large number of Network Management Stations 1b) Inadequate flow control - i.e. a station is continuously transmitting and not waiting for responses 1c) excessive broadcast traffic on the network segment. 2) Memory depletion due to excessive console output traffic Or, 3) a latent software defect or hardware failure. To eliminate these messages, use the "TM=mask" command to disable the traces.

RTL ISR=nn

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. The Ethernet controller caused an interrupt. Additional normal-completion indications may follow: "[Remote DMA complete]" "[TX ok]" "[RX ok]" "<get: b=nn-c=nn>".

[RTL RST]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. This unsolicited message is displayed when an unusual hardware or software condition is detected. The Ethernet controller was reset by software in response to a perceived error condition. Check the Ethernet segment to which the Management Module is attached for unusual conditions, such as a jabbering station. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the "TM=mask" command.

<RX>

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. A packet was extracted from the Ethernet receive queue. To eliminate these messages, use the "TM=mask" command to disable the traces. This message does not indicate an error condition. No corrective action is required.

[RX error]

This advanced debug message should be displayed only when debug traces have been enabled at the advice of TRANSITION Networks technical support. The unsolicited message is displayed when an unusual condition is detected by the Ethernet controller and indicates one of the following: 1) A packet with an invalid CRC was received. 2) A frame alignment error occurred. 3) A packet was missed (probably due to a peak in network load). The Ethernet controller is reset as a precaution. To eliminate this message, use the "TM=mask" command to disable the traces.

SCI: Serial console errors are occurring. Check cables and terminal.

This unsolicited message indicates that hardware errors are being encountered on the console's serial interface. Most commonly, this message is seen on the Telnet console, and is frequently accompanied by an inability to enter commands properly due to garbage characters appearing on the console. The most common cause for this is that a terminal is attached to the system's serial port, but is powered down. This can (depending on the construction of the hardware in the terminal) cause electrical conditions that can be mistaken for incoming (but flawed) serial data. Check to make sure that you have either nothing at all or a fully operational terminal with a properly wired null modem cable attached to the Management Module's serial port. If this is the case and the message persists, call TRANSITION Networks technical support for assistance.

Command-Line Interface - Messages

SNMP: berdecode - *ttttt*.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Decode of an incoming PDU failed. The PDU was discarded. *ttttt* provides a reason:

- “memory allocation failed” usually triggered by heavy network traffic and/or heavy console traffic. Unless this message is displayed frequently or system operation is impaired, no corrective action is required.
- “parent decode failed” occurs as SNMP attempts to clean up after an earlier error. Can be ignored.

The remaining messages indicate a malformed or incompatible incoming message:

- “Alignment failure” the expected length of some element of the message does not match the actual length.
- “invalid integer” an integer with a size other than 1, 2, or 4 bytes was received.
- “null OID” an Object ID had zero sub-identifiers.
- “illegal OID” indicates that a sub-identifier in an Object ID had more than 28 data bits.
- “invalid length” an octet string had zero data length, or a NULL had non-zero data length. This message is sometimes caused by an NMS transmitting a NULL community string. This is not supported by the Management Module.
- “undefined tag” an element of the message could not be identified.

SNMP: berdecode - Tag *nnnn* not defined

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the Management Module received an SNMP PDU that it could not decode. If the message persists, call TRANSITION Networks for assistance.

SNMP: berfree - tag *nnnn* not implemented

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

SNMP: beroutput - unimplemented tag *nnnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the Management Module received an SNMP PDU that it could not decode. If the message persists, call TRANSITION Networks for assistance.

SNMP: Cannot process request. Reason: *tttt*

This message is a response to a console command. The GET/GETNEXT/SET operation entered from the console could not be processed for the given reason. Check the MIB document for the variable you are attempting to access to make sure the Object ID you are entering is correct, and (for SET operations) that you understand the type and range of the variable correctly. Note that the appropriate security information is automatically supplied for all GET/GETNEXT/SET operations initiated from the console. The console must be in super-user mode before a SET operation is permitted. For values of *ttttt*, see message “SNMP: Error ‘*ttttt*’ error_index=*nnn* on request from *nnn.nnn.nnn.nnn*”

Also note that OIDs must be fully specified when using the GET and SET commands; all table indices must be specified or a trailing **.0** must be specified for non-tabular variable, e.g. **get = sysName.0**.

SNMP: Community is not OCTET STRING in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Decode of incoming PDU failed

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A variety of causes are possible, e.g. malformed SNMP message, out of memory, etc. Usually, this message is accompanied by other more specific messages, if the appropriate traces are enabled.

SNMP: dumpbertree - tag *nnnn* not implemented

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

SNMP: Error '*tttt*' error_index=*nnn* on request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The Management Module was unable to process an incoming SNMP request for the stated reason. The error index indicates which of the (possibly many) variable bindings (i.e. individual sub-requests) in the incoming message caused the error. Values for *tttt* include:

"noError" Theoretically impossible. If this message is displayed, contact TRANSITION Networks for assistance.

"tooBig" An incoming message or the response to that message was too large for the Management Module to handle. If this message persists, contact TRANSITION Networks for assistance.

"noSuchName=*tttt*" A request was received for an Object ID that is not supported by the Management Module, or the community name in the request is invalid. Make sure the correct community names and MIBs are loaded into the managing station. Another possible cause is that a SET request message attempted to change an item that is read-only in the current MIB view. (i.e. the data item is read-only in all MIB views, or the public community string was used for a SET operation on a read-write data item.)

"badValue" An incoming SET request had a variable binding with an SMI data type incompatible with that of the variable being changed (e.g. "sysName" cannot be set to an integer), or the data was excessively large.

"readOnly" Theoretically impossible. If this message is displayed, contact TRANSITION Networks for assistance.

"genErr" One of the following: 1) An incoming message contained an integer that was 3 bytes long or 5 or more bytes long 2) An incoming message contained an unrecognized BER data type. 3) Memory allocation failed while processing an SNMP message. 4) An incoming message contained an excessively long Object ID.

SNMP: Error displaying SNMP message

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Probably indicates a low-memory condition during the display of "outgoing SNMP" traces.

SNMP: [ERROR | ERROR CLEAR] trap transmitted to *nnn.nnn.nnn.nnn*.

This unsolicited message is displayed when a trap condition occurs. This message is printed only when the appropriate traces are enabled via the "TM=mask" command and traps are properly configured

SNMP: Error index is not 0 in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

Command-Line Interface - Messages

SNMP: Error index is not INTEGER in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Error status is not 0 in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Error status is not INTEGER in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Extra data in variable binding in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: GET [*nnn.nnn.nnn.nnn*] id=*nnnn* ind=*nnnn* *tttt* *nnn.nnn.nnn...*

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. It indicates that a variable binding is being processed by SNMP. The message that immediately follows shows the data associated with the binding. Note that one trace message is printed per binding; the id=*nnnn* given allows the user to determine which bindings were grouped in a single PDU. The text string *tttt*, if present, indicates an error code returned during processing of the binding. The remainder of the line is the object ID requested in the binding. This message is printed only when the appropriate traces are enabled via the "TM=mask" command.

SNMP: getlen - unimplemented tag *nnnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the Management Module received an SNMP PDU that it could not decode. If the message persists, call TRANSITION Networks for assistance.

SNMP: GETNEXT [*nnn.nnn.nnn.nnn*] id=*nnnn* ind=*nnnn* *tttt* *nnn.nnn.nnn...*

See "SNMP: GET id=..."

SNMP: Individual variable binding SEQUENCE missing in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Internal error, invalid backlink scanning slot *n*

This message indicates a latent software defect or a hardware defect. Power cycle the management module. If message persists, contact TRANSITION Networks for assistance.

SNMP: Internal error, invalid MIB structure

This is a system startup message. This message indicates a latent software defect. Call TRANSITION Networks for assistance.

SNMP: Invalid oid *tttt*

This message is a response to a console command. Either a symbolic OID (as in the Appendix) or a numeric Object ID with at least three sub-identifiers was expected (e.g. "1.3.6"). For GET and SET operations, a fully specified OID is required, i.e. all indices (for tables) or a trailing ".0" (for scalars) must be specified, even when the OID is specified symbolically.

SNMP: Invalid OID tag in variable binding in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Memory allocation error

This message is a response to a console command. Insufficient memory was available to process the request, usually due to a peak in system activity. Retry the operation. If the message persists, call TRANSITION Networks for assistance.

SNMP: Outer variable binding SEQUENCE missing in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: PDU from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An SNMP message has arrived from the IP address noted. If enough memory is available, a decode of the message will be displayed. This message is displayed only if the appropriate traces are enabled via the TM= command.

SNMP: PDU to *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An SNMP message is being transmitted to the IP address noted. If enough memory is available, a decode of the message will be displayed. This message is displayed only if the appropriate traces are enabled via the TM= command.

SNMP: Power supply #[1 | 2] is [UP | DOWN]. Trap sent to *nnn.nnn.nnn.nnn*.

This message is displayed either at system start up or as an unsolicited message during operation. It indicates that the operational status of one of the chassis' power supplies has changed and that a "POWER SUPPLY STATUS CHANGE" trap has been transmitted. It is normal for this message to be displayed during system startup if the chassis lacks its normal complement of two power supplies. This message is printed only when the appropriate traces are enabled via the "TM=mask" command and traps are properly configured.

SNMP: Request ID is not INTEGER in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: SET [*nnn.nnn.nnn.nnn*] id=*nnnn* ind=*nnnn* *tttt* *nnn.nnn.nnn...*

See "SNMP: GET id=..."

Command-Line Interface - Messages

SNMP: SNMP PDU is not SEQUENCE in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: system reset performed via SNMP from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The Management Module has been ordered (via an SNMP "SET" operation) to save all settings into FLASH (as if the SAVE command had been entered from the console) and reboot itself.

SNMP: Trap polling is now enabled.

This message indicates that the user has successfully enabled trap polling. As a result, the trap detection system has been re-initialized and the chassis slots are now being examined for new trap conditions. See also "SNMP: Warning: SNMP traps are disabled until..."

SNMP: Variable binding value is constructed in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Version is not INTEGER in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Unrecognized request tag *nnnn* in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call TRANSITION Networks for assistance.

SNMP: Version is not V1 in request from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A remote network management system (identified by its IP address) has attempted to communicate with the Management Module using a version of SNMP SMI other than V1. This version of the Management Module's software supports only SMI V1.

SNMP: Warning: SNMP traps are disabled until a manager address is defined via the SET TRAPMGR command and a trap poll interval is assigned via the TRAPPOLL command.

In order for trap polling to occur, the conditions mentioned in the message must be met. A parameter is 'defined' or 'assigned' when it is non-zero. These values must be saved via the 'SAVE' command or they will be lost during the next reboot, and trap polling will again be disabled.

[su] CPSMC1900>

This is a prompt that indicates that the Management Module's command line interface is ready for another super-user command. To return to non-privileged mode, enter the "SU" command.

NOTE: The console prompt string is determined by the MIB variable *mib2.system.sysName*. The default value for this MIB variable is CPSMC1900, as shown here. Changing the value of *mib2.system.sysName* will change the appearance of the console prompt.

Super-user mode off.

This message is a response to a console command. Super-user mode was disabled via the "SU" command. The default command set has been restored.

Super-user mode on.

This message is a response to a console command. Super-user mode was enabled via the "SU=password" command. Additional privileged commands are now available. See the help menu.

TCP: duplicate TCB in create_tcb nnnn,nnn.nnn.nnn.nnn,nnnn,nnn.nnn.nnn.nnn

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TCP: Incoming datagrams with invalid checksums are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a segment with an invalid TCP checksum is received, and for every 256 such datagrams after that. Unless this message is displayed frequently, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

TCP: insufficient resources in create_tcb

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TCP: Invalid cond in scmp

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TCP: invalid option. TCB=n

This unsolicited message is printed in response to a packet that arrived at the Ethernet interface. It indicates that an unrecognized option was seen on an incoming TCP segment, implying some sort of data corruption or protocol stack incompatibility. If the message persists, contact TRANSITION Networks for assistance.

TCP: Invalid state for CLOSE nnnnnnnn n

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

Command-Line Interface - Messages

TCP: Invalid TCP checksum, possibly from nnn.nnn.nnn.nnn port nnnn

TCP: checksum calculated=nnnn transmitted=nnnn ln=nnnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming TCP segment was invalid. This is usually due to the corruption of the datagram in transit. Note that the address displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. Unless this message is displayed frequently or system operation is impaired, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

TCP: Not initialized

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TCP_send fail n. tcb=nnnnnnnn buf=nnnnnnnn len=nnn state=n

This message may indicate a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TELNET: Change will become effective when this Telnet session ends.

Changes made via the "SET TNTRIP" or "SET TNTRIPMASK" commands take effect at the next *start* of a Telnet session, whether or not one is currently active.

TELNET: High-volume debug traces disabled. Old mask=nnnnnnnn

This message is displayed after a Telnet session with the management module is initialized. This is a notification that, due to reduced console throughput over Telnet, traces that are likely to cause large amounts of output have been disabled. Though it is not recommended, these traces may be re-enabled.

TELNET: An invalid login attempt was rejected. Password entered was:

This message is displayed on the console (serial) after an invalid attempt to log in to the Telnet server. A hexadecimal dump of the invalid password follows this message. The correct password is the private community string, and is case sensitive. The most common cause of an inability to complete a Telnet login is the use of a Telnet client that uses nonstandard TCP or Telnet options. Check for non-ASCII characters in the hexadecimal dump of the password, and look for other TCP or Telnet related error messages on the serial console. If either of these are found, try running your Telnet client in its simplest (i.e. most compatible) mode, or try using a different Telnet client. If neither of these are found, recheck that the password you are using is identical to the private community string. If you are still unable to log in, contact TRANSITION Networks technical support for assistance.

TELNET: open failed

This message indicates that the Telnet server's attempt to begin listening for an incoming TCP connection was unsuccessful. This may be an indication of a latent software defect. Power cycle the management module. If the message persists, contact TRANSITION Networks for assistance.

TELNET: Remote from nnn.nnn.nnn.nnn console disconnected.

This is a notification that an active Telnet console session has been terminated or that the Telnet server's network resources have been deallocated as part of reinitialization of the server, as happens when the Telnet security configuration is changed. An active session is terminated when the remote client actively disconnects from the management module's Telnet server, when the server is unable to contact the client, or when the LOGOFF command is entered.

TRANSMIT TIMEOUT

This unsolicited message is displayed when an unusual hardware or software condition is detected. The Ethernet controller did not confirm completion of a transmit command. This may indicate a hardware failure. Power cycle the Management Module. If the message persists, call TRANSITION Networks for assistance.

<TX>

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. An Ethernet transmit attempt was made. To eliminate these messages, use the "TM=mask" command to disable the traces.

[TX error]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of TRANSITION Networks technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that a transmit attempt was aborted due to excessive collisions. The Ethernet controller is reset as a precaution. To eliminate this message, use the "TM=mask" command to disable the traces.

UDP: Incoming datagrams with invalid checksums are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a datagram with an invalid UDP checksum is received, and for every 256 such datagrams after that. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

UDP: Invalid UDP checksum, possibly from *nnn.nnn.nnn.nnn* port *nnnn*

UDP: checksum calculated=*nnnn* transmitted=*nnnn* ln=*nn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming UDP datagram was invalid. This is usually due to the corruption of the datagram in transit. Note that the address and port displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

UDP: Unsupported destination port *nnn* from *nnn.nnn.nnn.nnn*

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The datagram is addressed to a service not supported by the Management Module. For example, if another station attempts to communicate with the UDP TFTP service on the Management Module, this message will be displayed since the Management Module does not support TFTP. The only supported port is SNMP. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. This message does not indicate an error condition. No corrective action is required.

UNEXPECTED EXCEPTION, SP=*nnnnnnnn* PC=*nnnnnnnn* SR=*nnnnnnnn*

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

Command-Line Interface - Messages

Usage: PING=nnn.nnn.nnn.nnn

This message is a response to a console command. This indicates a syntax error in the entry of a PING command. Enter "PING" to use the last valid PING address provided, or "PING=a.b.c.d" where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the command form "PING" is entered but no valid IP address has been entered via a previous "PING=a.b.c.d". This message is also displayed when the IP address 0.0.0.0 is entered. It is not possible to ping this address.

Use the SAVE command to make the current configuration permanent.

This message is a response to a configuration change made from the console or via SNMP. The configuration has changed since the last restart of the Management Module. The changes made will be lost the next time the Management Module is reset, rebooted, or power cycled - unless they are saved in FLASH memory as suggested. You must first enter super-user mode by entering the "SU=password" command to make the SAVE command accessible.

USER BREAK, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call TRANSITION Networks for assistance.

WARNING: Gateway IP address is undefined. (Use SET GATEWAY= *command*)

This message can be displayed at system startup and whenever the Management Module's IP parameters are changed via console command or SNMP PDU. The default value for the Management Module's gateway IP address is 0.0.0.0, which is invalid. A gateway IP address must be assigned to the Management Module before it can communicate with any station that is not on the same logical IP subnetwork.

WARNING: Local IP address is undefined. (Use SET IP= *command*)

This message can be displayed at system startup and whenever the Management Module's IP parameters are changed via console command or SNMP PDU. The default value for the Management Module's IP address is 0.0.0.0, which is invalid. An IP address must be assigned to the Management Module before it can be accessed via a management station.

WARNING: Local IP nnn.nnn.nnn.nnn and gateway IP nnn.nnn.nnn.nnn are not on the same subnet under subnet mask nnn.nnn.nnn.nnn

This message can be displayed at system startup and whenever the Management Module's IP parameters are changed via console command or SNMP PDU. This message indicates that the gateway is not on a locally attached network (i.e. the 'network' bits in the local IP address are not the same as the corresponding bits in the gateway address) and is therefore unreachable. This probably means that there has been an error configuring the local IP address, the gateway address, or the subnet mask. The most likely result of this is that all IP datagrams not destined for stations on the local subnet will be lost. To fix this problem, choose a local IP address, a gateway IP address, and a subnet mask that are compatible, and enter them into the system via the "SET IP=ip", "SET GATEWAY=ip", and/or "SET NETMASK=mask" commands, then enter the "SAVE" command to make the changes permanent.

WARNING: Saved configuration settings missing or corrupt.

This is a system startup message. This message is normal on a new Management Module or (sometimes) on a Management Module whose firmware has been updated. When this message appears, the Management Module's network interface is disabled. The user should (at a minimum) enter an IP address (via the "SET IP=ip" command), a subnet mask (via the "SET NETMASK=mask" command), and a gateway address (via the "SET GATEWAY=ip" command), then enter the "SAVE" command. If this procedure does not eliminate the message, call TRANSITION Networks for assistance.

WARNING: Subnet mask is undefined. (Use SET NETMASK= command)

This message can be displayed at system startup and whenever the Management Module's IP parameters are changed via console command or SNMP PDU. The default value for the Management Module's subnet mask is 0.0.0.0, which is invalid. A subnet mask must be assigned to the Management Module before it can communicate with any station that is not on the same logical IP subnetwork.

nnnnnnnn=nnnn
nnnnnnnn==nnnn

This is an advanced debug message that should be displayed only when debug traces have been enabled at the advice of TRANSITION Networks Technical Support. These messages show I/O operations to the Ethernet chip. At the left is the I/O address being read/written, at the right is the value being *read* (==) or *written* (=). To eliminate these messages, use the "TM=mask" command to disable the traces.

3.4.3 Command-Line Interface Trace Masks

The trace mask, set using the **TM=** command and always entered and displayed in hex, is the combination of all of the currently selected traces - each represented by a single bit.

To see a list of the available (and currently active) trace masks, at the command line interface, enter

?TM

Currently active trace masks are indicated by an asterisk.

NOTE: The default mask is hex 8101 - local SNMP trap condition + checksum + ICMP errors

Using trace masks (other than the default) is not recommended except on the specific advice of TRANSITION Networks Technical Support. Trace masks may impair the Management Module's operation due to the large amount of console output trace masks can cause if the network segment is carrying even light traffic.

NOTE: *When the console output queue (which holds roughly 30 lines of text by default) is full, new console messages are discarded without notice.*

4 MAINTENANCE & SERVICE

Maintenance direction for the TRANSITION Networks *PointSystem™*
Conversion Center™ provided in this section includes:

4.1	Fault Isolation and Recovery	4.2
4.1.1	At the Remote Network Management Station	4.2
4.1.2	At the Cabinet Front	4.4
4.2	Hardware Replacement Procedures	4.6
4.2.1	Replacing Media Converter Slide-In-Module	4.6
4.2.2	Replacing Management Module	4.7
4.2.3	Replacing AC Power Supply Module	4.8
4.2.4	Replacing 48-VDC Power Supply Module	4.10
4.2.5	Replacing 48-VDC Power Supply Module Fuse	4.13
4.2.6	Replacing AC Power Supply Module Fuse	4.15
4.3	Firmware Upgrades	4.16

All Installation and service must be performed by qualified service personnel.

4.1 Fault Isolation and Recovery

Fault isolation and recovery begins at the network location most convenient for the network administrator.

4.1.1 At the Remote Network Management Station

At the remote Network Management Station (NMS), use the installed SNMP network management software to validate the connection between the Network Management Station and the Media Conversion Center.

- **Determine if the Media Conversion Center is receiving but rejecting SNMP requests from the Network Management Station.**

Error messages from the SNMP management application such as “No Such Name,” “Read Only,” “Access Denied,” “Request Rejected” may indicate that the Media Conversion Center Management Module is receiving, but failing to process, requests from the SNMP management application. If the Management Module is receiving but rejecting the Manager’s requests, a configuration mismatch (possibly induced by changes at the Network Management Station) is indicated. Referring to documentation for the SNMP management application at the Network Management Station, install the correct MIB document into the SNMP management application. Enter the same community names into the SNMP management application and the Media Conversion Center Management Module.

- **Determine if the Network Management Station can display SNMP data from network devices other than the Media Conversion Center Management Module.**

Refer to documentation for the SNMP management application for the appropriate diagnostic method(s) to use to verify that Network Management Station access to the network has not been interrupted.

If Network Management Station access to the network has been interrupted, refer to documentation and/or technical support for the NMS.

- **Determine if the Network Management Station has an up-to-date map of the network (including DNS names, if applicable).**

Refer to documentation for the SNMP management application for appropriate diagnostic method(s) to use to verify that the DNS names and IP addresses for the DNS server, the SNMP management application at the Network Management Station, and the Media Conversion Center Management Module all match.

If the addresses do NOT match, refer to documentation for the DNS server, for the SNMP management application at the Network Management Station, and/or for the Media Conversion Center Management Module for direction for modifying the addresses to correct the discrepancy.

- **Determine if the Network Management Station can PING the Media Conversion Center Management Module.**

Refer to SNMP management application documentation for direction for entering the PING command and for specifying the DNS name of the Media Conversion Center Management Module.

If the PING is successful, SNMP traffic may be blocked by a router or firewall or the fault may be in the SNMP management application. Check configuration of all network devices between Management Station and the Management Module to ensure that none are filtering SNMP traffic. Recheck configuration and operation of the SNMP management application.

If PING reports that a DNS name is invalid, the Network Management Station may be unable to reach the DNS server because of an incorrect Network Management Station configuration, a network fault, or a problem with the DNS server. Try PINGing the Media Conversion Center Management Module IP address instead of the DNS name. If this works, investigate possible problem with Network Management Station DNS configuration, a mismatch between the IP address in the Media Conversion Center Management Module and the entry in the DNS server, or some other problem with the DNS server.

- **Determine if the Network Management Station can PING other stations on the same IP subnet as the Media Conversion Center Management Module.**

Refer to documentation for the SNMP management application for direction for entering the system PING command and specifying the IP address or DNS name of an IP station on the same IP subnet as the Media Conversion Center Management Module.

If the PING is successful, SNMP traffic may be blocked by a router or firewall or by a fault in the SNMP management application.

If the PING fails, investigate an invalid IP configuration in the SNMP management application.

NOTE: An incorrect subnet mask may permit access to some, but not all, of a remote subnet.

- **Determine if a station on the same IP subnet as the Media Conversion Center Management Module can PING the Media Conversion Center Management Module.**

Referring to the station's networking utilities documentation, enter the PING command, specifying the IP address or DNS name of the Media Conversion Center Management Module.

If the PING is successful, investigate an invalid subnet mask and/or gateway address in the Media Conversion Center Management Module IP configuration.

If the PING fails, look for a fault other than between the SNMP management application and the Media Conversion Center.

4.1.2 At the Cabinet Front

At the Media Conversion Center, examine the hardware and connections.

Determine if RESET corrects the problem.

Press the RESET button on the Media Conversion Center Management Module and observe the results.

Determine if the Media Conversion Center is receiving power.

Inspect power LED indicators at the front of the Media Conversion Center. At least one of the two **In Use** LED indicators should be illuminated. If not, check the **Power** LED indicator on the power supply installed at the rear of the Media Conversion Center.

Failure may indicate:

- Loss of AC power at outlet
- Unplugged unit
- Power switch OFF
- Failed fuse
- Power supply not seated in slot
- Failed power supply.

If fuses blow repeatedly, have the AC outlet inspected by a qualified electrician. If no **Power** or **In Use** LED indicators on the front of the chassis are illuminated but **Power** LED indicators on the rear of the chassis are illuminated, unplug the power supply from the AC outlet, pull it out of its slot and re-seat it. If these and the other obvious corrective actions fail, contact TRANSITION Networks Technical Support.

Determine if the Management Module is receiving power.

Verify that the Management Module **Power** LED indicators are illuminated.

Failure may indicate:

- Management Module not properly seated in slot
- Management Module failure
- Media Conversion Center failure.

If reseating the Management Module in the chassis slot does not cause the **Power** LED indicator to be illuminated, contact TRANSITION Networks Technical Support.

4 MAINTENANCE & SERVICE

Determine if the Media Conversion Center Management Module is connected to an active 10BASE-T Ethernet port.

NOTE: On a network that is too quiet, this test will not be possible.

The **RX** LED indicator should blink every time a network broadcast is transmitted. The **TX** LED indicator should blink every time the Management Module responds.

Failure may indicate that Media Conversion Center Management Module connection to the network has failed.

Verify the integrity of the 10BASE-T hub/switch port into which the Media Conversion Center Management Module is attached and of the 10BASE-T twisted pair Ethernet cable that leads from the hub/switch to the Media Conversion Center Management Module.

If a network tester is not available, verify the network path by unplugging the Ethernet cable from the back of the Media Conversion Center Management Module and plugging the cable into a replacement station (such as a PC – not a hub or a switch) to verify network connectivity. If the 10BASE-T replacement station can communicate with the network and the TX and RX LED indicators on the Media Conversion Center Management Module still do not respond when the same cable is attached, contact TRANSITION Networks Technical Support.

4.2 Hardware Replacement Procedures

WARNING: The CPSMC1900 series 19-Slot Media Conversion Center contains no user-serviceable parts. DO NOT, UNDER ANY CIRCUMSTANCES, open and attempt to repair 19-Slot Media Conversion Center equipment. Failure to observe this warning could result in personal injury and/or death from electrical shock.

NOTE: Failure to observe the above warning will immediately void any warranty.

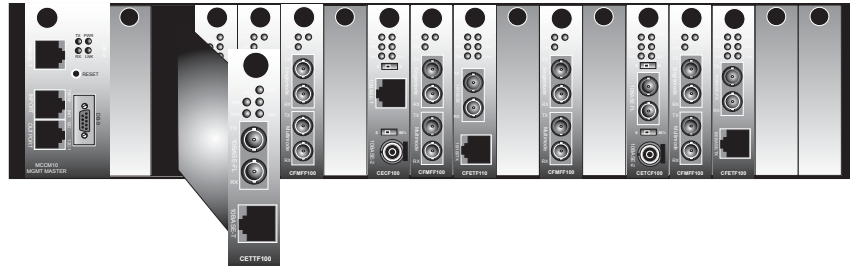
4.2.1 Replacing Media Converter Slide-In-Module

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when replacing Media Converter Slide-in-Module(s). Failure to observe this caution could result in damage to, and subsequent failure of, the Media Converter Slide-in-Module(s).

NOTE: The Media Converter Slide-in-Modules are hot-swappable.

To replace a Media Converter Slide-in-Module in the CPSMC1900 chassis:

1. Remove Media Converter Slide-in-Module to be replaced by loosening one (1) screw that secures Slide-in-Module to CPSMC1900 chassis front and sliding Media Converter Slide-In-Module from CPSMC1900 chassis.
2. Align replacement Media Converter Slide-in-Module with Media Conversion Center installation slot so that panel fastener screw is at top of Management Module.
3. Carefully slide replacement Media Converter Slide-in-Module into



installation slot.

NOTE: Ensure that Media Converter Slide-in-Module is firmly seated against backplane.

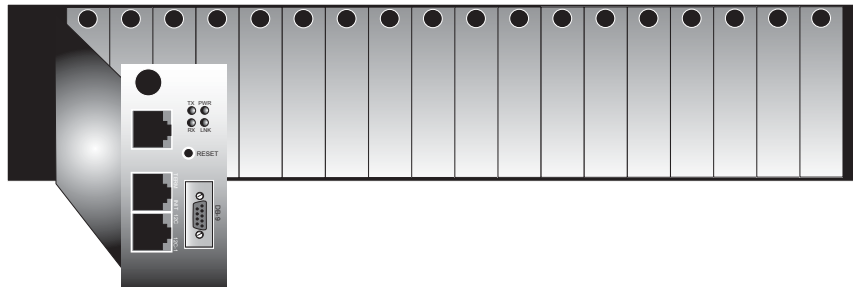
4. Install replacement Media Converter Slide-in-Module by carefully rotating attached panel fastener screw clockwise to secure Media Converter Slide-in-Module to CPSMC1900 chassis.

4.2.2 Replacing Management Module

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when replacing Management Module in the 19-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Management Module.

NOTE: Management Modules can be “hot-swapped”.

NOTE: One (1) *Base Management Module* (2-slot CPSMM-200 or 1-slot CPSMM-120) must be installed in the primary – or only – managed CPSMC1900 Media Conversion Center. One (1) *Expansion Management Module* (CPSMM-210) may be installed in any secondary managed CPSMC1900 Media Conversion Center(s).



NOTE: Though Management Module(s) can be installed in any Media Conversion Center slot, use of the leftmost installation slots for installing Management Module(s) is recommended in order to keep cascading cables separate from network cables installed on Media Converter Slide-In-Modules.

To replace a Management Module in the CPSMC1900 chassis:

1. At Media Conversion Center front, remove Management Module to be replaced by loosening panel screw that secures Management Module to CPSMC1900 and sliding Management Module from CPSMC1900 chassis.
2. Align Management Module with Media Conversion Center installation slot so that panel fastener screw is at top of Management Module.
3. Carefully slide Management Module into installation slot, aligning Management Module with installation guides.

NOTE: Ensure that Management Module is firmly seated against backplane.

4. Rotate attached panel fastener screw clockwise to secure Management Module to CPSMC1900 chassis.

NOTE : After installation of a replacement Base Management Module, *PointSystem™* network management must be re-configured. (See 2.10.2.)

4.2.3 Replacing AC Power Supply Module

WARNING: DO NOT CONNECT POWER SUPPLY MODULE TO AC POWER BEFORE INSTALLING IN MEDIA CONVERSION CENTER. FAILURE TO OBSERVE THIS CAUTION COULD RESULT IN EQUIPMENT DAMAGE AND/OR PERSONAL INJURY OR DEATH.

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when replacing Power Supply Module in the 19-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Power Supply Module.

To replace a Power Supply Module in the CPSMC1900 chassis:

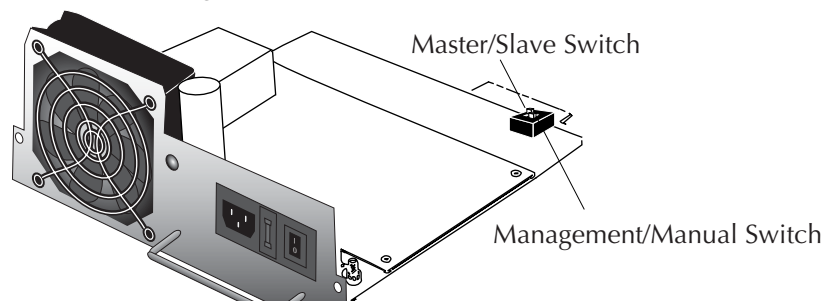
Remove Faulty Power Supply Module from Chassis

1. Set Power Supply Module power switch to **0**.
2. Disconnect outlet end of power cord from AC wall socket.
3. *At Media Conversion Center back*, disconnect power cord from power receptacle of Power Supply Module to be replaced.
4. Remove Power Supply Module to be replaced by removing two (2) screws that secure Power Supply Module to CPSMC1900 chassis and sliding Power Supply Module from chassis.

NOTE: Retain screws for installing replacement Power Supply Module.

Set Replacement Power Supply Module Master/Slave-Management/Manual Switch

The CPSMC1900 Power Supply Module is shipped with a set of Master/Slave-Management/Module switches installed on the circuit board.



The **MASTER/SLAVE** switch allows the Power Supply Module to be configured as the primary (master) or as the secondary (slave) Power Supply Module. As primary (master), the Power Supply Module provides power to the chassis and all installed Slide-In-Cards, unless prevented from doing so due to external power source failure. As secondary (slave), the Power Supply Module waits in stand-by, ready to supply power to the chassis on primary (master) power source failure.

The **MANAGEMENT/MANUAL** switch allows TRANSITION Networks PointSystem™ software to control the primary (master) or secondary (slave) Power Supply Module setting AND TO OVER-RIDE THE PHYSICAL MASTER/SLAVE SWITCH SETTING ON THE POWER SUPPLY MODULE.

NOTE: When the MANAGEMENT/MANUAL switch is set to MANAGEMENT, the default MASTER/SLAVE configuration is primary (master) unless changed, at the software interface, to secondary (slave).

4 MAINTENANCE & SERVICE

CAUTION: When installing two Power Supply Modules, AT LEAST ONE Power Supply Module MUST BE CONFIGURED AS PRIMARY (master). Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module(s).

CAUTION: In a 0-60° C environment, TWO POWER SUPPLIES MUST BE INSTALLED AND THE POWER SUPPLIES MUST BE CONFIGURED FOR LOAD-SHARING: one Power Supply Module must be configured as primary (master) and one Power Supply Module must be configured as secondary (slave). Failure to observe this caution could result in data transfer failure and/or damage to, and subsequent failure of, Power Supply Module(s).

1. Set MASTER/SLAVE switch, if necessary.
To configure the Power Supply Module as the primary (master) Power Supply Module, set MASTER/SLAVE switch to position labeled "MASTER". To configure the Power Supply Module as the secondary (slave) Power Supply Module, set MASTER/SLAVE switch to position labeled "SLAVE".
2. Set MANAGEMENT/MANUAL switch, if necessary.
To allow *PointSystem™* software to over-ride the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled "MANAGEMENT". To prevent *PointSystem™* software from over-riding the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled "MANUAL".

Install Replacement Power Supply Module in Chassis

1. Carefully slide replacement Power Supply Module into installation slot, aligning Power Supply Module with installation guides:
NOTE: Ensure that the Power Supply Module is firmly seated against the chassis backplane.
2. Carefully install two (2) retained screws through Power Supply Module into Media Conversion Center chassis, rotating clockwise to secure.

Connect to External Power

1. Connect female end of power cord to power receptacle on Power Supply Module.
2. Plug male end of power cord into correct voltage AC rack or wall socket.
3. Set Power Supply Module power switch to **I**.
4. Verify that Media Conversion Center is powered by observing illuminated Power LED and fan operation.

4.2.4 Replacing 48-VDC Power Supply Module

Read and follow all warning notices and instructions marked on the product or included in the manual

All installation and service must be performed by qualified service personnel.

This product is intended to be used in a restricted access location. Connect the product to a -48VDC SELV (Safety Extra Low Voltage) supply that is electrically isolated from the DC Source. The -48 VDC source is to be reliably connected to earth (ground). Equipment grounding is vital to ensure safe operation.

Prior to installation, use a voltmeter/ohmmeter to check the wiring for the presence of earth ground.

A readily accessible disconnect device as part of the building installation shall be incorporated into the fixed wiring. The disconnect device (a -48 VDC, 15 or 20A circuit breaker or switch) must be included in the ungrounded supply conductor. Overcurrent protection must be a 15 or 20A, -48 VDC fuse or circuit breaker.

WARNING: DO NOT CONNECT POWER SUPPLY MODULE TO POWER BEFORE INSTALLING IN MEDIA CONVERSION CENTER. FAILURE TO OBSERVE THIS CAUTION COULD RESULT IN EQUIPMENT DAMAGE AND/OR PERSONAL INJURY OR DEATH.

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when replacing Power Supply Module in the 19-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Power Supply Module.

To replace a Power Supply Module in the CPSMC1900 chassis:

Remove Faulty Power Supply Module from Chassis

1. Set 48-VDC Power Supply Module power switch to **0**.
2. Disconnect +48-VDC terminal from Media Conversion Center terminal block control marked "+" by turning terminal screw counter-clockwise.
3. Disconnect -48-VDC terminal from Media Conversion Center terminal block control marked "-" by turning terminal screw counter-clockwise.
4. Disconnect ground terminal from Media Conversion Center terminal block control marked "chassis ground" by turning terminal screw counter-clockwise.
5. Remove Power Supply Module to be replaced by removing two (2) screws that secure Power Supply Module to CPSMC1900 chassis and sliding Power Supply Module from chassis. Retain screws for installing replacement Power Supply Module.

Set Replacement Power Supply Module Master/Slave-Management/Manual Switch

The CPSMC1900 Power Supply Module is shipped with a set of Master/Slave-Management/Module switches installed on the circuit board.

*The **MASTER/SLAVE** switch allows the Power Supply Module to be configured as the primary (master) or as the secondary (slave) Power Supply Module. As primary (master), the Power Supply Module provides power to the chassis and all installed Slide-In-Cards, unless prevented from doing so due to external power source failure. As secondary (slave), the Power Supply Module waits in stand-by, ready to supply power to the chassis on primary (master) power source failure.*

*The **MANAGEMENT/MANUAL** switch allows TRANSITION Networks PointSystem™ software to control the primary (master) or secondary (slave) Power Supply Module setting AND TO OVER-RIDE THE PHYSICAL MASTER/SLAVE SWITCH SETTING ON THE POWER SUPPLY MODULE.*

NOTE: When the MANAGEMENT/MANUAL switch is set to MANAGEMENT, the default MASTER/SLAVE configuration is primary (master) unless changed, at the software interface, to secondary (slave).

CAUTION: When installing two Power Supply Modules, AT LEAST ONE Power Supply Module MUST BE CONFIGURED AS PRIMARY (master). Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module(s).

NOTE: If both Power Supply Modules are configured as the primary (master) Power Supply Module, each Power Supply Module contributes a portion of the power to the chassis (“load sharing”).

AC and DC Power Supply Modules are not intended to load share when used concurrently. When operating a Conversion Center with an AC Power Supply Module in one slot and a DC Power Supply Module in the other, both Supplies may not be set to ‘Primary’ (i.e., master).

1. Set MASTER/SLAVE switch, if necessary.

To configure the Power Supply Module as the primary (master) Power Supply Module, set MASTER/SLAVE switch to position labeled “MASTER”. To configure the Power Supply Module as the secondary (slave) Power Supply Module, set MASTER/SLAVE switch to position labeled “SLAVE”.
2. Set MANAGEMENT/MANUAL switch, if necessary.

To allow PointSystem™ software to over-ride the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled “MANAGEMENT”. To prevent PointSystem™ software from over-riding the physical MASTER/SLAVE switch setting, set MANAGEMENT/MANUAL switch to position labeled “MANUAL”.

Install Replacement Power Supply Module in Chassis

1. Carefully slide replacement Power Supply Module into installation slot, aligning Power Supply Module with installation guides:

NOTE: Ensure that the Power Supply Module is firmly seated against the chassis backplane.

2. Carefully install two (2) retained screws through Power Supply Module into Media Conversion Center chassis, rotating clockwise to secure.

Connect to Power

CAUTION: Ensure that power source is NOT powered and that 48-VDC power ON/OFF switch is set to “O” when connecting to Power Supply Module. Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module.

1. Connect +48-VDC terminal to Media Conversion Center terminal block control marked “+”. Turn terminal screw clockwise to secure.
2. Connect -48-VDC terminal to terminal block control marked “-”. Turn terminal screw clockwise to secure.
3. Connect ground terminal to Media Conversion Center terminal block control marked “**chassis ground**”. Turn terminal screw clockwise to secure.
4. Set 48-VDC Power Supply Module power switch to **I**.
5. Verify that Media Conversion Center is powered by observing illuminated Power LED and fan operation.

4.2.5 Replacing 48-VDC Power Supply Module Fuse

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when replacing the 48-VDC fuse in the 48-VDC Power Supply Module. Failure to observe this caution could result in damage to, and subsequent failure of, the 48-VDC Power Supply Module.

CAUTION: Replace fuse only with same size and rating. Failure to observe this caution could result in equipment damage.

To replace a 48-VDC Power Supply Module fuse:

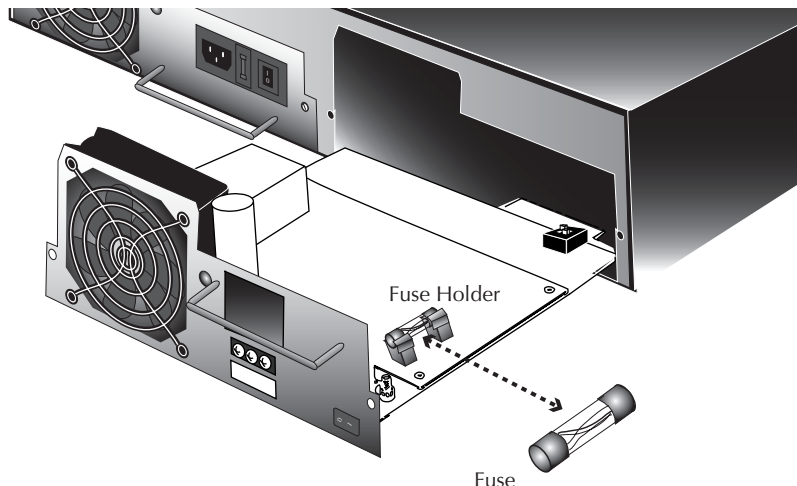
Remove Power Supply Module from Chassis

1. Set 48-VDC Power Supply Module power switch to **0**.
2. Disconnect +48-VDC terminal from Media Conversion Center terminal block control marked "+" by turning terminal screw counter-clockwise.
3. Disconnect -48-VDC terminal from Media Conversion Center terminal block control marked "-" by turning terminal screw counter-clockwise.
4. Disconnect ground terminal from Media Conversion Center terminal block control marked "chassis ground" by turning terminal screw counter-clockwise.
5. Remove Power Supply Module by removing two (2) screws that secure Power Supply Module to CPSMC1900 chassis and sliding Power Supply Module from chassis.

NOTE: Retain screws for re-installing Power Supply Module.

Replace Fuse on Power Supply Module Circuit Board

1. Locate fuse on 48-VDC Power Supply Module.



2. Carefully remove fuse from fuseholder.
3. Install **same size and rating** replacement fuse in fuse holder.

Replace Power Supply Module in Chassis

1. Carefully slide replacement Power Supply Module into installation slot, aligning Power Supply Module with installation guides:

NOTE: Ensure that the Power Supply Module is firmly seated against the chassis backplane.

2. Carefully install two (2) retained screws through Power Supply Module into Media Conversion Center chassis, rotating clockwise to secure.

Connect to Power

CAUTION: Ensure that power source is NOT powered and that 48-VDC power ON/OFF switch is set to "O" when connecting to Power Supply Module. Failure to observe this caution could result in damage to, and subsequent failure of, Power Supply Module.

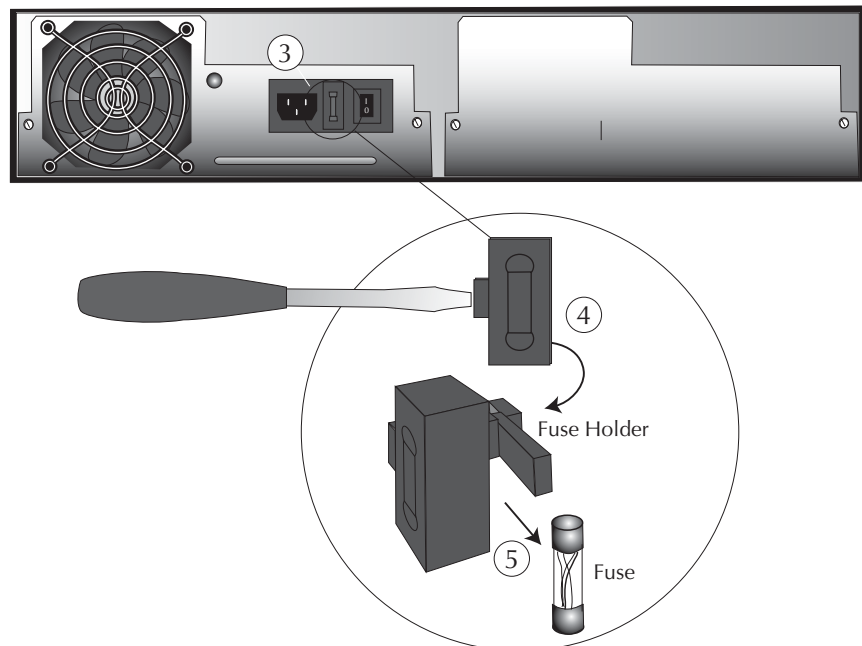
1. Connect +48-VDC terminal to Media Conversion Center terminal block control marked "+". Turn terminal screw clockwise to secure.
2. Connect -48-VDC terminal to Media Conversion Center terminal block control marked "-". Turn terminal screw clockwise to secure.
3. Connect ground terminal to Media Conversion Center terminal block control marked "chassis ground". Turn terminal screw clockwise to secure.
4. Set 48-VDC Power Supply Module power switch to I.
5. Verify that Media Conversion Center is powered by observing illuminated Power LED and fan operation.

4.2.6 Replacing AC Power Supply Module Fuse

CAUTION: Replace fuse only with same size and rating. Failure to observe this caution could result in equipment damage.

To replace an AC Power Supply Module fuse:

1. Set Power Supply Module power switch to **0**.
2. Disconnect outlet end of power cord from AC wall socket.
3. *At Media Conversion Center back*, disconnect power cord from Power Supply Module power receptacle.
4. From inside edge of power receptacle, insert small flat blade screwdriver into groove on front inside edge of fuse holder and carefully pry fuse holder (with installed fuse) from Power Supply Module.



5. Rotate fuse holder to display fuse.
6. Carefully remove fuse from fuse holder.
7. Install **same size and rating** replacement fuse in fuse holder.
8. Return fuse holder and fuse to installation position in Power Supply Module.
NOTE: Snap fuse holder into place.
9. Connect power cord to Power Supply Module power receptacle.
10. Connect power cord to AC wall socket.
11. Set Power Supply Module power switch to **I**.
12. Verify that POWER LED at front of 19-Slot Media Conversion Center is illuminated.

4.3 Firmware Upgrades

CAUTION: The CPSMC1900 software cannot check to ensure that the firmware is compatible with installed hardware. Incorrect firmware downloads **WILL** damage the Management Module, **NECESSITATING FACTORY SERVICE**. If in doubt, abort the upgrade and contact **TRANSITION Networks Technical Support** for assistance.

CAUTION: If the 'WRITE' phase is interrupted or fails for any reason, the Management Module will be damaged, **NECESSITATING FACTORY SERVICE**. Use of a battery-backed uninterruptible power supply is **HIGHLY recommended**.

NOTE: The Management Module's firmware can be upgraded only via the serial port.

NOTE: The firmware download command "XR" is unavailable when a telnet session is active.

NOTE: Firmware upgrade may cause all saved settings to be lost.

NOTE: Do NOT transfer a ZIP file. UnZIP the ZIP file and transfer the binary file contained in the ZIP file. (Firmware files are NOT automatically extracted from ZIP files.)

To upgrade the firmware:

1. Obtain new firmware by contacting **TRANSITION Networks Technical Support**.
2. Initiate the CPSMC1900 end of X-modem transfer by entering the following commands at the CPSMC1900 command-line prompt:

`CPSMM100> SU=<case sensitive password>`

`[SU] xr`
3. Enter terminal emulator-specific commands to initiate the terminal emulator end of the X-modem transfer and to cause the file to be transferred.

NOTE: When file transfer is complete, the new code is written into flash memory and the Management Module reboots.

NOTE : After the firmware upgrade, *PointSystem™* network management may require re-configuration. (See 2.10.2.)

Appendix A. PointSystem™ Technical Specifications

Dimensions

Chassis

17" x 14.3" x 3.5"
(430 mm x 363 mm x 89 mm)

Power Supply Modules

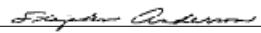
8.3" x 8.4" x 2.7"
(211 mm x 214 mm x 69 mm)

Media Converter Modules

3.4" x 0.86" x 5.0"
(86 mm x 22 mm x 127 mm)

Base Management Module

3.4" x 1.7" x 5.0"
(86 mm x 43 mm x 127 mm)

TRANSITION NETWORKS		DECLARATION OF CONFORMITY
Name of Mfg:	Transition Networks 6475 City West Parkway, Minneapolis MN 55344 USA	
Model:	PointSystem™ Media Conversion Center	
Part Number:	CPSMC1900-100	
Regulation:	EMC Directive 89/336/EEC	
Purpose:	To declare that the PointSystem™ Media Conversion Center to which this declaration refers is in conformity with the following standards. EMC-CISPR 22: 1985 Class A; EN 55022: 1988 Class A; EN 50082-1:1992; EN 60950 A4:1997; IEC 801.2, IEC 801.3, and IEC 801.4; IEC 950	
<i>I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).</i>		
 Stephen Anderson, Vice-President of Engineering		<u>September 14, 2001</u> Date

Shipping Weight

Chassis

17.5 Lbs

Power Input

CPSMP200

Universal Input 100-240V 50/60Hz 3.0-1.5 A

AC Input:

TN P/N	Requirement	Location
3344	120 volts, 60 hertz	USA/Canada/Mexico
3344	100 volts, 50-60 hertz	Japan
3347	230 volts, 50 hertz	Europe
3348	240 volts, 50 hertz	Australia
3349	240 volts, 50 hertz	United Kingdom

CPSMP210

48V DC 2.75 A Max

Power Distribution

CPSMP200

Power supply modules supply +12VDC at 9A maximum. (+12VDC at 9A is the maximum the chassis can supply to all front converters because only one supply provides power. The other is used if the first fails.) Each converter can draw a maximum of +12VDC at 0.3A.

CPSMP210

With 48VDC connected to the CPSMP210 module input terminal block, the power supply module will supply 12VDC at 12.5A maximum. Input Power: 48VDC at 2.75A typical (with fully loaded chassis); Output Power: 12VDC at 12.5A maximum

Environment

Temperature*:	0-50°C (32° to 122° F)
Storage Temperature:	-20 to 85°C
Humidity	10-90%, non condensing
Altitude	0-10,000 feet

*Refer to the power consumption data for EACH model Media Converter Slide-in-Module (provided in User's Guide shipped with Media Converter Slide-in-Module) to determine optimum site configuration.

Compliance

UL listed EN60950; FCC & CISPR class A; CE Mark

Warranty

Lifetime

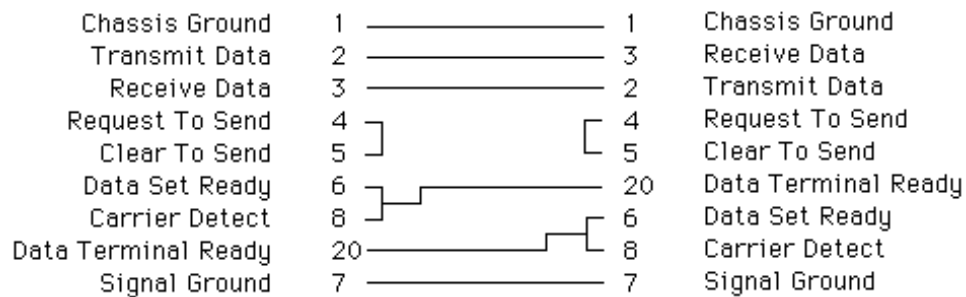
Appendix B. Null Modem Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Media Conversion Center Management Module to access the command-line interface.

The table below shows the pin assignments for the DB9 cable.

Function	Mnemonic	Pin
Carrier Detect	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

25 Pin RS-232 Null Modem Cable



Appendix C. Introduction to SNMP in the CPSMC1900

NOTE: A protocol is a set of rules that governs data transmission and reception. The Simple Network Management Protocol (SNMP) is an Internet protocol (as are protocols such as the Transmission Control Protocol (TCP) and Internet Protocol (IP)). SNMP was developed in the mid-1980's as an interim response to communication barriers encountered among different types of networks. Formally specified in a series of related Request for Comment (RFC) documents, SNMP is becoming the de facto Internet network management standard.

SNMP is a protocol that defines network communication between a **Managed Device** (such as the CPSMC1900) and the network administrator at a **Network Management Station**. The SNMP protocol uses simple **Operations** on a set of variables on the managed device (called instances of **Managed Objects**) to allow the network administrator to monitor and to control the managed device from a remote location.

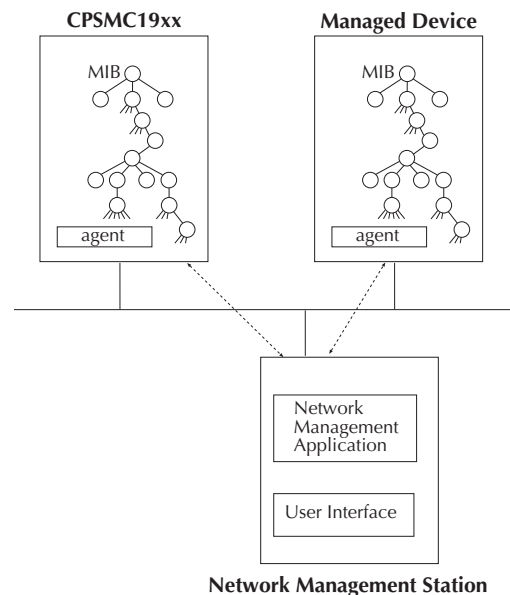
Managed Device A managed device is a hardware unit with embedded SNMP software (including a **Management Information Base (MIB)** – the set of managed objects on that managed device – and an **agent** – the software that monitors the data in the MIB) connected to a network with SNMP management available.

NOTE: An CPSMC1900 with installed Media Converter Modules, and with an installed Management Module, is a single managed device.

Network Management Station (NMS) A network management station (NMS) is a high-end workstation, also connected to the network, that provides **SNMP network management application software** and a **user interface**. *NOTE: An optional network management application and user interface for the CPSMC1900 are provided by SNMPc™ software from CastleRock Computing installed on a network Windows™ PC.*

SNMP Operations SNMP is a simple *request-response* protocol with four defined operations: GET, GET-NEXT, SET, and TRAP. To monitor (read) the managed device, the network administrator initiates, through the user interface to the network management application on the NMS, the GET and GET-Next operations on selected called instances of managed objects (variables) in the managed device MIB. To control (write) the managed device, the network administrator initiates, through the user interface to the network management application on the NMS, the SET operation on selected instances of managed objects in the managed device MIB. The SNMP agent on the managed device initiates the trap operation to alert the network administrator, through the user interface to the network management application on the NMS, of instances of MIB-defined asynchronous events on the managed device.

Managed Objects Managed objects are the types of information on a managed device that can be identified and collected by SNMP agent software and that can be made available to the network administrator through the user interface on the NMS. Managed objects can be scalar (a single object instance – such as the CPSMC1900 network IP address) or tabular (related instances – such as the various LED displays on a Media Converter Module installed in the CPSMC1900).



MIBs and Object Identifiers

The Management Information Base (MIB) is the set of managed objects on a managed device and is depicted as an abstract tree with unnamed root, as shown in the diagram.

Managed Objects are depicted as nodes in the MIB tree. Object identifiers (object IDs, or OIDs) for the Managed Objects use a machine-independent format (a subset of the Abstract Syntax Notation 1 (ASN.1)) to uniquely identify each managed object in the MIB tree. NOTE: Abstract notation allows communication among diverse networks.

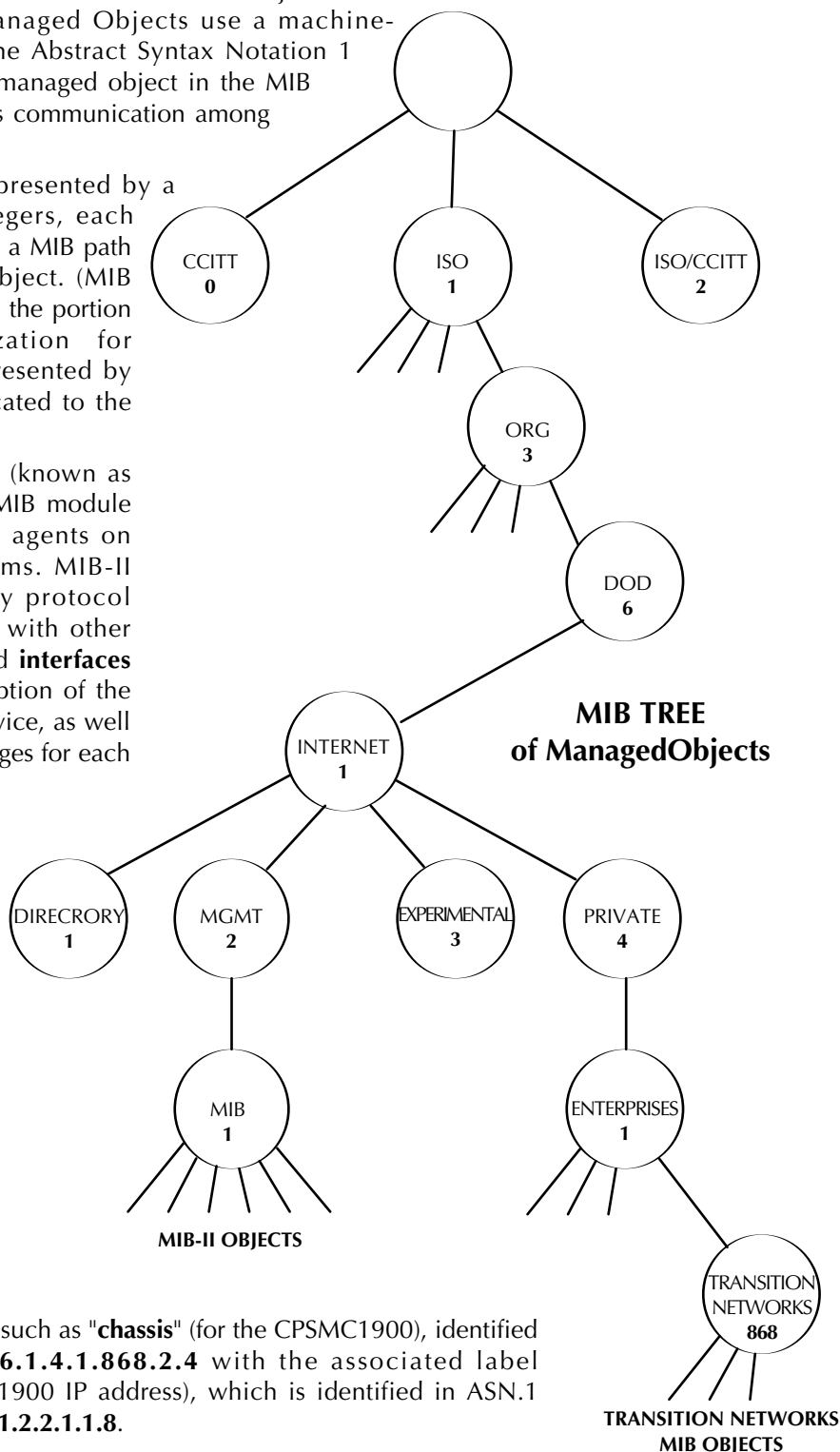
OIDs in the ASN.1 syntax are represented by a structured series of positive integers, each separated by a period, that “follows” a MIB path to uniquely identify a managed object. (MIB development is particularly active in the portion of the International Organization for Standardization (ISO) branch represented by object identifier **1.3.6.1** and dedicated to the Internet community.)

The current Internet-standard MIB (known as MIB-II, with OID **1.3.6.1.2.1**) is a MIB module typically supported by all SNMP agents on TCP/IP enabled devices or systems. MIB-II contains 171 objects grouped by protocol (including TCP, IP, UDP, SNMP), with other identifiers, including **system** (1) and **interfaces** (2). This MIB file contains a description of the object hierarchy on the managed device, as well as the OID, syntax and access privileges for each variable in the MIB.

The network administrator can use an OID: **1.3.6.1.2.1.1** to identify MIB II “system description” data to an SNMP agent. The network administrator also can use the associated label, **sysDescr**, to identify the same data to the SNMP agent, since the SNMP agent uses the MIB-II object identifier: **1.3.6.1.2.1.1.1 = sysDescr** to translates the label to the corresponding OID.

Vendors define private branches to include instances of their products. Transition Networks' private MIB is represented by the object identifier

1.3.6.1.4.1.868 and includes objects such as “**chassis**” (for the CPSMC1900), identified in ASN.1 notation by OID **1.3.6.1.4.1.868.2.4** with the associated label “**cpsmm100IPAddress**” (the CPSMC1900 IP address), which is identified in ASN.1 notation by OID **1.3.6.1.4.1.868.2.4.1.2.2.1.1.8**.



Appendix D. Displaying the CPSMC1900 MIB

Though the list of supported MIB variables changes as firmware is upgraded, the Management Module CLI contains a OID-to-text translation table which serves as a list of the MIB variables supported by any given firmware revision. Using the “?” command, the MIB list can be displayed in its entirety or can be searched by OID or variable name.

Displaying MIB Variables

Example 1: Displaying names and OIDs of all MIB variables related to a media converter

NOTE: Each media converter-related MIB variable has a prefix that is simply the media converter model name with all case and punctuation data removed.

To display names and OIDs of all MIB variables related to the CFETF100:

```
CPSMM100 > ?=cfetf100
```

The associated MIB values are listed, as in this example:

```
cfetf100Id = 1.3.6.1.4.1.868.1.4.1.2.4
cfetf100FiberLink = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.10
cfetf100Fault = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.11
cfetf100FastLinkPulse = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.12
cfetf100Enabled = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.13
cfetf100Pause = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.14
cfetf100LinkPassThrough = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.15
cfetf100AutoCross = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.16
cfetf100TPActivity = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.17
cfetf100FiberActivity = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.18
cfetf100ConfigMode = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.19
cfetf100BiaIndex = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.1
cfetf100SlotIndex = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.2
cfetf100Groups = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.3
cfetf100CfgMatch = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.5
cfetf100SerialNumber = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.6
cfetf100ConnA = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.7
cfetf100ConnB = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.8
cfetf100TPLink = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.9
```

Example 2: Displaying the names and OIDs based on string

To display names and OIDs of all MIB variables containing the string: LINK:

```
CPSMM100> ?=link
```

The associated MIB values are listed, as in this example:

```
cpsmm100EthernetLink = 1.3.6.1.4.1.868.2.4.1.2.2.1.1.14
cettf100FiberLink = 1.3.6.1.4.1.868.2.4.1.2.2.3.1.10
cettf100LinkPassThrough = 1.3.6.1.4.1.868.2.4.1.2.2.3.1.15
cettf100TPLink = 1.3.6.1.4.1.868.2.4.1.2.2.3.1.9
cfetf100FiberLink = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.10
cfetf100FastLinkPulse = 1.3.6.1.4.1.868.2.4.1.2.2.4.1.12
```

Example 3: Displaying names and OIDs of related items

To display the names and OIDs of all items in the mib-2.system group

```
CPSMM100> ?=1.3.6.1.2.1.1
```

The associated MIB values are listed, as in this example:

```
sysDescr = 1.3.6.1.2.1.1.1
sysObjectID = 1.3.6.1.2.1.1.2
sysUpTime = 1.3.6.1.2.1.1.3
sysContact = 1.3.6.1.2.1.1.4
sysName = 1.3.6.1.2.1.1.5
sysLocation = 1.3.6.1.2.1.1.6
sysServices = 1.3.6.1.2.1.1.7
```

Displaying the Entire MIB Tree

NOTE: The example assumes that the system prompt and private community string have not been changed from their default values.

To display the entire MIB table:

Enter “superuser” mode:

```
CPSMM100> su=private
```

Super-user mode on.

Use the “sql” command to temporarily increase the amount of buffer space available for console output.

```
[su] CPSMM100> sql=20000
```

Serial queue limit changed from 2000 to 20000 bytes

Enter the “?=” command to search the MIB entries for a period.

```
[su] CPSMM100> ?=.
```

Every MIB entry contains a period, so all system MIB variables are listed.

```
sysDescr = 1.3.6.1.2.1.1.1
sysObjectID = 1.3.6.1.2.1.1.2
. . . . .
cpsSlotPwrState = 1.3.6.1.4.1.868.2.4.2.2.3.2.1.3
cpsIsPrimary = 1.3.6.1.4.1.868.2.4.2.2.3.3
```

After the MIB has been displayed, return “sql” to the default value. Failure to do this may result in impaired system performance.

```
[su] CPSMM100> sql=2000
```

Serial queue limit changed from 20000 to 2000 bytes

Exit “superuser” mode:

```
[su] CPSMM100> su
```

```
CPSMM100>
```

Super-user mode off.

Appendix E. SNMP GLOSSARY

ARP	Address Resolution Protocol Method for determining Ethernet address from IP address.
binding	See 'variable binding.'
flash	Memory that retains its contents when power is disconnected.
MIB	Management Information Base. The types, names, and OID tree structure of a group of SNMP variables. Manifested in software on the managed network entity and in a text document for the managing station. [The objects that are available in a managed system. The information is represented in Abstract Syntax Notation 1 (ASN.1)]
ICMP	Internet Control Message Protocol. A set of information, error, and control messages used on IP networks. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.
IP	Internet Protocol. A network layer protocol whose primary responsibility is routing.
Object Id	A "name" for a particular piece of SNMP data. for example, a GET operation on the object id "1.3.6.1.2.1.1.1.0" returns a string describing the managed system. This same OID is used for every system that supports the system description variable. The dotted numeric value is used instead of a simple text name so that a tree structure can be implied in the name.
OID	Object ID See above.
get	An SNMP 'read' operation in which the data associated with a specific, exact object id is returned.
getnext	An SNMP 'read' operation where the data returned is the data associated with the object id that is numerically 'next.' e.g. a GETNEXT operation on the object id 1.3.6.1.2.1.1.1.0 would return the Object ID 1.3.6.1.2.1.1.2.0 and the data associated with it.
PDU	Protocol Data Unit. An SNMP operation encoded for network transmission.
Protocol	The formal set of rules on coding, formatting and timing of inputs and outputs between communicating devices.
set	An SNMP 'write' operation.
SNMP	Simple Network Management Protocol An application layer protocol that allows remote management of networked devices.
SMI	Structure of Management Information.
UDP	User Datagram Protocol. A connectionless transport layer protocol used in IP networks; provides an end-to-end interface for use by applications. This protocol carries SNMP as a payload, and is carried as a payload by IP.
variable binding	A subsection of a PDU. A variable binding contains an Object ID and the data value associated with that Object ID.
XMODEM/CRC	A protocol commonly used to transfer files across an RS-232 link.

Appendix F. Power Consumption Data Sheet

Typical *PointSystem*TM Device Power Consumption

The table below lists the typical power consumption of the individual Slide-in-Module devices that are used with the CPSMC *PointSystem*TM Conversion Center.

Slide-in-Module Media Converter	Typical Power Volt • Amps (Watts)
Base Chassis w/ Power Supply and Fan	6.5 W
Management Module	3.3 W
Expansion Module	2.4 W
2nd Power Supply	5.0 W
2nd Fan Module	4.5 W
CBFTF – 10/100Base-TX to 100Base-FX (6 port)	5.0 W
CBFTF – 10/100Base-TX to 100Base-FX(2 port)	4.0 W
CCSFC – Two (2) BNC ports to Fiber	4.5 W
CDFTF – 100Base-TX to 100Base-FX	6.8 W
CETCT – 10Base-T to 10Base-2	2.4 W
CETTF – 10Base-T to 10Base-FL	2.3 W
CFETF – 100Base-TX to 100Base-FX	3.5 W
CFETF – 100Base-TX to (Fiber) 100Base-FX	2.5 W
CFMFF – Singlemode to Multitmode (all types)	3.3 W
CGETF – 1000Base-T to 1000Base-SX/LX Fiber	5.5 W
CPSVT – Copper to Fiber	5.0 W
CSDTF – RJ-45 or BNC to/from Fiber (T1/E1)	3.7 W
CSETF – 10/100Base-TX to 10/100Base-SX	3.6 W

VAC Power Considerations

Available Power at three temperature ranges

The tables below list the available power for the PointSystem™ Base Chassis (with an installed VAC Power Supply Module) at three temperature ranges: 0-40°C, 0-50°C, and 0-60°C. Note how the available power decreases as the temperature range increases.

PointSystem™ Chassis With Installed AC Power Supply Module

Power from the Base Chassis available for the devices →	Site Ambient Temperature		
	0 – 40°C	0 – 50°C	0 – 60°C *
	110 W	82 W	55 W

Sample VAC Power Requirements

The PointSystem™ Base Chassis with one Management Module provides installation space for up to sixteen (16) Media Converter Slide-In-Modules. However, depending on the Slide-In-Modules selected, or the temperature range of the Chassis, there may not be sufficient power for all sixteen devices.

The following table lists the power requirements for a PointSystem™ chassis with 16 CFETF “TX-FX” modules. Note the power requirements at three different temperature ranges. This example includes an efficiency error of 0.7 (for VAC power calculations) and assumes a 20% margin of error.

Note that only at the 0-40°C temperature range is there enough power available for all 16 CFETF “TX-FX” modules. At 0-50°C and 0-60°C, the lower available power (and the required second power supply for the 0-60°C range) make using all 16 modules impossible at these temperature ranges.

Temperature Range	0 - 40°C	0 - 50°C	0 - 60°C*
Base Chassis	6.5 W	6.5 W	6.5 W
Management Module	3.3 W	3.3 W	3.3 W
2 nd Power Supply*	n/a	n/a	5.0 W
16 CFETF “TX-FX” modules (16 x 2.5 W = 40.0 W)	40.0 W	40.0 W	40.0 W
Subtotal	49.8 W	49.8 W	54.8 W
VAC correction (<i>divide by 0.7</i>)	71.1 W	71.1 W	78.3 W
Error (<i>add 20%</i>)	+ 14.2 W	+ 14.2 W	+ 15.6 W
Corrected Power Req.	85.3 W	85.3 W	93.9 W
Available Power	110.0 W	82.0 W	55.0 W

(*Installation of a second Power Supply Module is optional for operation at 0-40°C or 0-50°C, but is required for operation at 0-60°C.)

VDC Power Considerations

Available Power at three temperature ranges

The tables below list the available power for the PointSystem™ Base Chassis (with an installed VDC Power Supply Module) at three temperature ranges: 0-40°C, 0-50°C, and 0-60°C. Note how the available power decreases as the temperature range increases.

PointSystem™ Chassis With Installed 48-VDC Power Supply Module

Power from the Base Chassis available for the devices →	Site Ambient Temperature		
	0 – 40°C	0 – 50°C	0 – 60°C *
	90 W	72 W	55 W

Sample VDC Power Requirements

The PointSystem™ Base Chassis with one Management Module provides installation space for up to sixteen (16) Media Converter Slide-In-Modules. However, depending on the Slide-In-Modules selected, or the temperature range of the Chassis, there may not be sufficient power for all sixteen devices.

The following table lists the power requirements for a PointSystem™ chassis with 16 CFETF “TX-FX” modules. Note the power requirements at three different temperature ranges. This example includes an efficiency error of 0.7 (for VAC power calculations) and assumes a 20% margin of error.

Note that at the 0-40°C and the 0-50°C temperature ranges is there enough power available for all 16 CFETF “TX-FX” modules. At 0-60°C, the lower available power, and the required second power supply, make using all 16 modules impossible at this temperature range.

Temperature Range	0 - 40°C	0 - 50°C	0 - 60°C*
Base Chassis	6.5 W	6.5 W	6.5 W
Management Module	3.3 W	3.3 W	3.3 W
2 nd Power Supply*	n/a	n/a	5.0 W
16 CFETF “TX-FX” modules (16 x 2.5 W = 40.0 W)	40.0 W	40.0 W	40.0 W
Subtotal	49.8 W	49.8 W	54.8 W
VDC correction (divide by 0.85)	58.6 W	58.6 W	64.5 W
Error (add 20%)	+ 11.7 W	+ 11.7 W	+12.9 W
Corrected Power Req.	70.3 W	70.3 W	77.4 W
Available Power	90.0 W	72.0 W	55.0 W

(*Installation of a second Power Supply Module is optional for operation at 0-40°C or 0-50°C, but is required for operation at 0-60°C.)

